様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２９　年　　６　月　１８　日現在

機関番号：　１２６０８
研究種目：　若手研究(B)
研究期間：　2015～2016
課題番号：　１５Ｋ１６００２

研究課題名（和文）DNSSECの電子署名検証をリゾルバ分散により端末で高速・安全に実現する研究

研究課題名（英文）A Study of Client Based Efficient and Secure DNSSEC Validation By Resolver Separation

研究代表者

金　勇（JIN, YONG）

東京工業大学・学術国際情報センター・特任助教

研究者番号：６０７２５７８７

交付決定額（研究期間全体）：（直接経費）　　2,500,000円

研究成果の概要（和文）：平成27年度では、主に端末によるDNSSEC検証の負荷調査とシステムの設計及び実装を行なった。性能実験では端末の合計性能が更に高くなる可能性について確認できた。次に、DNSSEC検証のエラー処理機能を含む端末によるDNSSEC検証システムの実装及び機能評価を行なった。
平成28年度では、初年度の成果を国際会議で発表し、ローカル及び実環境で評価した成果を含めて論文誌に投稿し採択された。また、端末での名前解決のキャッシュ機能を有効化する方法を提案し、その成果を研究会で発表した。更に、端末でDNSSEC検証を行う際にリゾルバを分散して使う方法を検討し、プロキシで実現可能であることを確認した。

研究成果の概要（英文）：In the first year, we compared the performance of client based full resolver based DNSSEC validation and confirmed that the total performance of the clients can be higher than that of full resolver. Then we designed and implemented a client based DNSSEC validation system including the alert feature which can tell the user about the detail errors regarding to the failures of DNSSEC validation.
In the second year, first, we presented the achievement of the performance evaluation and implementation of the client based DNSSEC validation system in an international conference and also submit its corresponding revised version including the evaluation in the local as well as real network environment to a journal and achieved the acceptance. Moreover, we proposed a multithreading method on a client for the DNSSEC validation and presented it in a domestic conference. Finally, we also confirmed the possibility of resolver separation for the client based DNSSEC validation by using a proxy.

研究分野：　通信ネットワーク技術

キーワード：　client based DNSSEC　DNSSEC with alert　DNSSEC performance　Resolver separation

１．研究開始当初の背景

日々増加するグローバルドメイン名（2013年度に２．７億超）の数とインターネットサービスに対応する為に、名前解決の効率化を図る「キャッシュ DNS サーバ」(フルリゾルバ)の利用が一般的だが、フルリゾルバを狙うセキュリティ脅威も高まっている。それに対する一つの対策として DNSSEC が提案され、公開鍵暗号化と電子署名技術を利用して権威サーバとフルリゾルバ間で DNS 応答の完全性を提供する。しかし、DNSSEC の導入には以下の問題が生じている。

1. DNSSEC 署名検証により組織フルリゾルバの負荷が高くなる。
2. DNSSEC 署名検証を行う為に問合せ数と DNS トラフィクが増える。
3. DNSSEC はフルリゾルバと端末間は考慮しない。

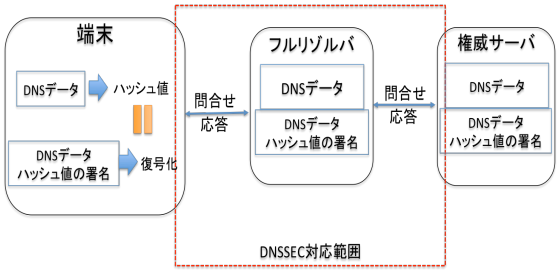

図１　DNSSEC の概要と適応範囲

図１のように、フルリゾルバから問合せを受けた際に、権威サーバは DNS レコードのハッシュ値を暗号化した電子署名を対応の DNS 応答に添付して返すが、フルリゾルバは受信した DNS 応答の電子署名を検証(ハッシュ値計算、復号化など)するために対応の公開鍵とその電子署名を取得する必要がある。このような DNSSEC 署名検証の負荷とそのために必要となる DNS トラフィックの増加が主な原因で、2014 年現在インターネット全体で DNSSEC 署名検証を行う名前解決の割合が僅か 12.08%(引用文献[1])に止まり、普及の進捗が進まない状況である。更に、DNSSEC ではフルリゾルバと端末間の DNS 応答の完全性を考慮してないため、セキュリティ脅威の最終目標である端末での対策が求められている。

２．研究の目的

DNS(Domain Name System)はインターネットにおいて欠かせない名前解決システムになっているが、DNS を悪用したセキュリティ脅威が高まりつつあり、その対策の一環として DNSSEC(DNS Security Extensions)が提案されている。しかし、DNS フルリゾルバ(以降フルリゾルバ)の負荷と DNS トラフィックの増加問題で導入がなかなか進んでない。また、DNSSEC での対策範囲は権威サーバとフルリゾルバ間であり、端末までは考慮してない。そこで本研究では、端末での DNSSEC における電子署名検証(以降 DNSSEC 署名検証)と利用するフルリゾルバの分散による安全かつ効率的な前解決機構の確立を目的とする。本研究での成果は、DNSSEC の普及促進と名前解決に伴うセキュリティ脅威の抑制に貢献が期待できる。

３．研究の方法

本研究の目的を達成するために、まず端末での DNSSEC 署名検証の負荷を調査しその実現性を示す。その後、端末への DNSSEC 署名検証機能の追加と DNSSEC 署名検証の効率化を行う。

具体的には、まず既に提案されている端末による DNSSEC 署名検証手法(引用文献[2])と異なり、名前解決用のライブラリ改造を検討し汎用の DNSSEC 署名検証機能を開発する。

次に、端末に設定した２台のフルリゾルバを同時に利用して DNSSEC 署名検証に必要な情報(DNS レコードと電子署名)を速く取得することにより、DNSSEC 署名検証の効率化を図る。

最後に、提案手法のプロトタイプシステムを構築して実験環境において機能評価及び性能評価を実施し、次に実環境での評価を実施する。

４．研究成果

(1) 平成 27 年度では、主に端末による DNSSEC 署名検証の負荷調査及び既存問題の解決の実現性を確認するために、端末による DNSSEC 署名検証とフルリゾルバによる DNSSEC 署名検証の性能比較実験と簡単な端末による DNSSEC 署名検証機能の導入を行った。まず、3 台の端末にそれぞれ別途リゾルバをインス

トールして端末での DNSSEC 署名検証実験を行い、既存のフルリゾルバを使った DNSSEC 検証と性能比較を行った。その結果、図 2 に示しているようにフルリゾルバと端末上でキャッシュを一切使わない状況では、2 台以上の端末を同時に使う場合端末の合計性能がフルリゾルバを上回ることが確認できた。

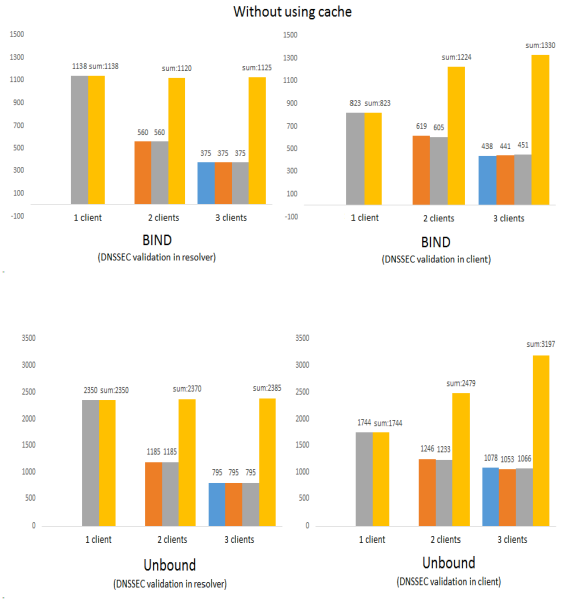

図 2 キャッシュ無しの DNSSEC 検証比較

また、キャッシュ機能を使う例として一部の問合せに対してキャッシュを使った状況では、図 3 に示しているように 3 台の端末を同時に使う場合端末の合計性能がフルリゾルバを上回ることが確認できた。これらの結果はフルリゾルバを使う主な理由であるキャッシュ機能を使わない場合はともかく、キャッシュ機能を使う場合でもキャッシュの利用割合によって端末の合計性能が更に高くなる可能性を示している。

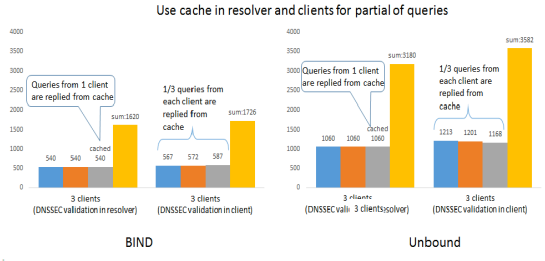

図 3 キャッシュ機能を一部利用した場合の DNSSEC 検証比較

次に、端末に DNSSEC 署名検証機能を導入するために、DNSSEC 署名検証のエラー処理を具体化する方法を提案し、実装及び機能評価を行った。既存の DNSSEC 署名検証では、DNSSEC を導入してないドメインの場合や DNSSEC 署名検証に必要な鍵の設定問題で検証が失敗した場合、同じ SERVFAIL エラーを返すため、ユーザはその区別ができないとともに名前解決ができない問題がある。そのため、そのエラーの種類を具体化し、DNSSEC を導入してない場合や DNSSEC 署名検証が失敗した場合に名前解決結果を返すと共にユーザにそのことを伝えるシステムを提案した。その結果、図 4 に示しているように、端末上で DNSSEC 署名検証を行い、署名検証に失敗した場合や DNSSEC を導入してない場合でも名前解決の結果をユーザに返し、警告メッセージに基づいてユーザがその利用について判断可能なことが確認できた。

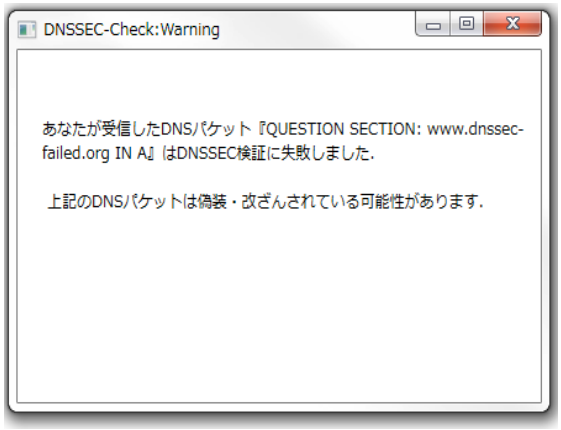

図 4 DNSSEC 検証失敗の警告メッセージ

(2) 平成 28 年度では、まず初年度に行った端末による DNSSEC 署名検証とフルリゾルバによる DNSSEC 署名検証の性能比較実験の成果を国際会議にて発表した。次に、ローカル及び実環境で機能を評価し、その成果も含めて論文誌に投稿し採択された。それから、端末での DNSSEC 検証性能を向上させるために、端末での名前解決のキャッシュ機能を有効化する方法を提案し、その成果を国内研究会にて発表を行った。さらに、端末で DNSSEC

検証を行う際にリゾルバを分散して使う方法を検討し、端末にプロキシを導入することで名前解決と DNSSEC 検証のための問合せを２つリゾルバに分けることが可能であることを確認した。今後この成果を国際会議などで発表する予定である。

<引用文献>

[1] DNSSEC Statistics, Internet Society.
http://www.internetsociety.org.
[2] DNSSEC-Trigger, NLnet Labs. http://www.nlnetlabs.nl.

５．主な発表論文等

〔雑誌論文〕（計 1 件）

[1]Yong Jin, Kunitaka Kakoi, Nariyoshi Yamai, Naoya Kitagawa and Masahiko Tomoishi, “ A Client Based DNSSEC Validation System with Adaptive Alert Mechanism Considering Minimal Client Timeout, ” IEICE Transactions on Information and Systems, Special Section on Information and Communication System Security, (Accepted and to be appeared in August,2017.)（査読有）

〔学会発表〕（計 5 件）

[1] K. Kakoi, Y. Jin, N. Yamai, N. Kitagawa and M. Tomoishi, ″Cache Function Activation on A Client Based DNSSEC Validation and Alert System by Multithreading,″ 2017 IEEE 41th Annual Computer Software and Applications Conference (COMPSAC), Torino, Italy, July 2017.（査読有）(To be appeared)

[2] Y. Jin, M. Tomoishi and N. Yamai,″An advanced client based DNSSEC validation and preliminary evaluations toward realization,″ 2016 International Conference on Information and Communication Technology Convergence (ICTC),Jeju,October 2016, pp.178-183.（査読有）

[3] K. Kakoi, Y. Jin, N. Yamai, N. Kitagawa and M. Tomoishi, ″Design and Implementation of a Client Based DNSSEC Validation and Alert System,″ 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC), Atlanta, GA, June 2016, pp.8-13.（査読有）

[4] 中村将也，栫邦雄，金勇，山井成良，北川直哉，友石正彦：マルチプロセス DNSSEC 検証システムのマルチスレッド化によるキャッシュ機能有効化，情報処理学会インターネットと運用技術研究会研究報告，2017-IOT-36, pp.1-6, カルチャーリゾート フェストーネ、沖縄、 2017 年 3 月.（査読無）

[5] 栫邦雄，金勇，山井成良，北川直哉，友石正彦：端末上で動作する DNSSEC 検証及び警告システムの設計と実装，情報処理学会インターネットと運用技術研究会研究報告,No.2016-IOT-33, pp.1-8, とりぎん文化会館（鳥取県立県民文化会館）、2016 年 5 月.(査読無)

６．研究組織

(1)研究代表者

金 勇（Jin, Yong）
東京工業大学・学術国際情報センター・特任助教
研究者番号：60725787