DNS 回答信頼度算出システムの実装と実環境への影響評価

Implementation of a DNS Response Reliability Estimation System
and Evaluation of its Influence on Real Environments

馬場 達也† 日下 貴義† 山岡 正輝† 松田 栄之†
Tatsuya Baba Takayoshi Kusaka Masaki Yamaoka Shigeyuki Matsuda
e-mail: {babatt, kusakat, yamaokam, matsudasg}@nttdata.co.jp

1. はじめに

DNS（Domain Name System）は、インターネット上のホストの名称と IP アドレスを対応付ける重要なシステムである。利用者は、DNS から回答された IP アドレスを正しいものと信じて、その IP アドレスの WWW サーバ等にアクセスをしている。しかし、ネームサーバを乗っ取り、利用者を不正な WWW サーバ等に誘導して個人情報を取得する等の行為も発生し、問題となっている。

そこで著者らは、名前解決時に、ローカルネームサーバから問い合わせ先のネームサーバに対してチェックを行うことにより、その結果から DNS 回答の信頼度を算出し、ユーザに通知する仕組みを提案してきた [1]。本稿では、提案した方式をプロトタイプとして実装し、実環境に適用した場合の影響について評価した結果を報告する。

2. 信頼度算出のためのチェック問い合わせ

著者らが提案している方式では、図 1 のように、クライアントが信頼度算出機能付ローカルネームサーバに対して名前解決の要求を行うと、信頼度算出機能付ローカルネームサーバが外部のネームサーバに対して通常の名前解決を行う。さらに、問い合わせ先ネームサーバに対して信頼度チェックのための問い合わせを行い、その結果から名前解決結果の信頼度を算出し、クライアントに通知する。

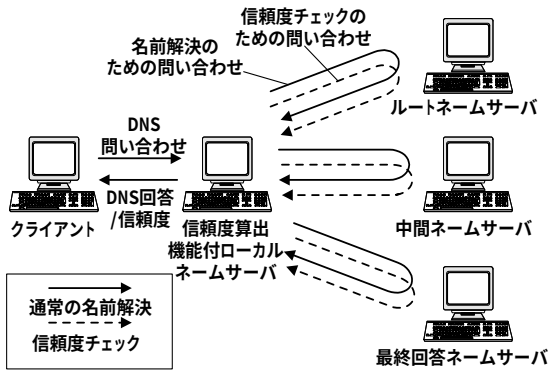

図 1 DNS 信頼度チェック方式

信頼度チェックのための問い合わせは、通常の DNS プロトコルを使用するため、外部のネームサーバが特別なプロトコルに対応する必要はない。信頼度算出機能付ローカルネームサーバが発行する DNS 問い合わせをまとめると表 1 の通りとなる。

†（株）NTT データ 技術開発本部
Research and Development Headquarters
NTT DATA CORPORATION

表 1 ローカルネームサーバから行う DNS 問い合わせ

問い合わせの種類（略称）	問い合わせ先
通常問い合わせ（QUERY）	ルートサーバから反復問い合わせ
BIND バージョン問い合わせ（NS-VERSION）	各ネームサーバ
ゾーン名をキーとした ANY 問い合わせ（ZONE-ANY）	各ネームサーバ
問い合わせ先のネームサーバのホスト名をキーとした ANY 問い合わせ（NS-ANY）	各ネームサーバ
ゾーン転送問い合わせ（ZONE-AXFR）	各ネームサーバ
問い合わせ先のネームサーバの IP アドレスをキーとした逆引き問い合わせ（NS-PTR）	各ネームサーバのアドレス毎にルートサーバから反復問い合わせ
解決した IP アドレスをキーとした逆引き問い合わせ（WWW-PTR）	ルートサーバから反復問い合わせ
名前解決を行ったドメイン名をキーとした ANY 問い合わせ（WWW-ANY）	最終回答ネームサーバ

3. DNS 回答信頼度算出システムの実装

信頼度算出機能付ローカルネームサーバは、BIND 9.2.1 をベースに実装した。信頼度チェックのための DNS 問い合わせは、通常の名前解決終了後、スレッドを使用して外部ネームサーバに並列に問い合わせるようにし、信頼度の算出は、すべての信頼度チェックの回答が得られた後に行うようにした。

また、クライアントでは、ユーザが直感的に信頼度を確認できるように、算出された信頼度およびチェック結果を表示するための GUI を、Microsoft Internet Explorer のツールバーとして実装した（図 2）。

図 2 DNS 回答信頼度表示ツールバー

4. 実環境への影響度に関する評価

本方式では、名前解決を行う際に、名前解決のための問い合わせとは別に、信頼度チェックのための問い合わせも行う。このため、この信頼度チェックのための問い合わせによってどの程度 DNS のトラフィックが増加するのか、作成したプロトタイプを使用して評価を行った。

4.1 評価方法

チェック問い合わせによって生じるトラフィック量（パケット数およびバイト数）を gov, edu, com, net, org, jp の各ドメインの Web サーバ（375 台）の名前解決を行うことで取得した。また、同時に、信頼度を算出するために要した時間を取得した。

4.2 評価環境

評価に使用した環境を図 3 に示す。また、信頼度算出機能付ローカルネームサーバのスペックを表 2 に示す。

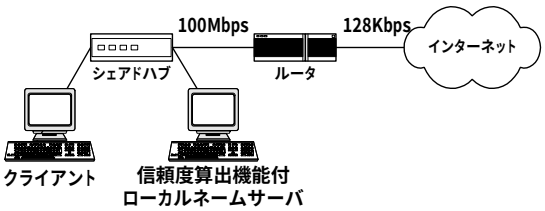

図 3 評価環境

表 2 ローカルネームサーバのスペック

OS	Red Hat Linux 9（カーネル 2.4.20）
CPU	Intel Pentium III 1GHz
メモリ	512MB
NIC	3Com 3C920（100Mbps）

4.2 評価結果

すべてのチェック問い合わせを有効にした場合に生じたトラフィックの平均は表 3 の通りとなった。また、チェック問い合わせのうち、ゾーン転送問い合わせ（ZONE-AXFR）とネームサーバ逆引き問い合わせ（NS-PTR）を無効とした場合のトラフィックの平均は表 4 の通りとなった。そして、信頼度チェック問い合わせおよび信頼度算出処理に要した時間は表 5 の通りとなった。

表 3 全てのチェック問い合わせを有効にした場合に発生したトラフィック（平均）

問い合わせ名称	パケット数（%）	バイト数（%）
QUERY	10.59 (3.52%)	1512.48 (1.77%)
NS-VERSION	8.73 (2.90%)	624.83 (0.73%)
ZONE-ANY	8.81 (2.92%)	2094.03 (2.45%)
NS-ANY	8.81 (2.93%)	1427.65 (1.67%)
ZONE-AXFR	99.80 (33.14%)	52133.82 (60.89%)
NS-PTR	154.35 (51.25%)	26495.86 (30.95%)
WWW-PTR	8.05 (2.67%)	1074.34 (1.25%)
WWW-ANY	2.01 (0.67%)	253.02 (0.30%)
計	301.14 (100%)	85616.03 (100%)

表 4 ZONE-AXFR および NS-PTR 問い合わせを無効にした場合に発生したトラフィック（平均）

問い合わせ名称	パケット数（%）	バイト数（%）
QUERY	11.19 (10.28%)	1571.88 (8.94%)
NS-VERSION	7.76 (7.13%)	565.90 (3.22%)
ZONE-ANY	8.36 (7.68%)	1937.06 (11.02%)
NS-ANY	9.01 (8.28%)	1466.49 (8.34%)
WWW-PTR	70.49 (64.77%)	11786.67 (67.04%)
WWW-ANY	2.01 (1.85%)	252.91 (1.44%)
計	108.83 (100%)	17580.06 (100%)

表 5 信頼度算出に要した時間（平均）

	問い合わせ	信頼度算出
すべての問い合わせを有効	10.373 秒	0.210 秒
ZONE-AXFR と NS-PTR を無効	4.284 秒	0.194 秒

5. 考察

すべてのチェック問い合わせを有効にした場合に生じたトラフィック量は、通常の問い合わせのみを行った場合と比較して、パケット数で 28.4 倍、バイト数で 56.6 倍となった。このトラフィック量の増加は、ZONE-AXFR および NS-PTR の 2 つの問い合わせが主な原因となっている。ネームサーバ側でゾーン転送を許可する設定になっていた場合には、大量のゾーン情報が転送されるため、トラフィックが異常に高くなる。また、逆引き問い合わせは、他のチェック問い合わせと異なり、ルートネームサーバから反復問い合わせを行う必要があるため、その分トラフィックが多く発生している。

信頼度チェックによるトラフィックの増加を少なくするためには、信頼度の算出への影響が小さいチェック問い合わせを無効とする必要がある。ZONE-AXFR と NS-PTR の 2 つの問い合わせは、ネームサーバのゾーン転送の設定と、ネームサーバのアドレスおよびホスト名の整合性を知るために行われるものであり、無効とした場合の信頼度の算出への影響は比較的小さい。ZONE-AXFR と NS-PTR を無効とした場合に生じるトラフィック量は、通常の問い合わせのみの場合と比較して、パケット数で 9.7 倍、バイト数で 11.2 倍に抑えることが可能となり、この 2 つのチェック問い合わせを無効とすることで、実環境への影響を小さくすることが可能となる。

また、信頼度の算出にかかる処理時間は、すべてのチェック問い合わせを有効にした場合で 10.6 秒、ZONE-AXFR と NS-PTR を無効とした場合で 4.5 秒となった。信頼度の算出処理は、名前解決完了後に行っているため、アクセス先の Web 画面が表示されるまでの時間には影響しない。このため、得られた処理時間は、実際の利用では問題のない範囲であると考えられる。

6. まとめ

本稿では、ローカルネームサーバから外部のネームサーバに対して信頼度チェックを行うことにより、DNS 回答の信頼度を算出する方式をプロトタイプとして実装し、実環境に適用した場合の影響について評価した結果を示した。評価の結果、ZONE-AXFR および NS-PTR 問い合わせを無効とすることで、実環境に大きな影響を与えることなく、本方式が適用可能であると判断した。

謝辞

本研究は、通信・放送機構（TAO）の委託研究テーマ「次世代 DNS に関する研究開発」の一環として行われているものである。

参考文献

[1] 馬場, 日下, 山岡, 松田, “DNS における信頼性情報付与のためのチェック方式の検討”, FIT2002 情報科学技術フォーラム 一般講演論文集 ⑷, pp.235-236, 2002 年 9 月.