M-101　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

A Study of a Method for Estimating Reliability of DNS Responses

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: {baba, kusaka, yamaoka, matu}@rd.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が回答した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、個人情報等を入力している。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。

このような問題に対して、利用者が安全にDNSを利用するために、DNS回答の信頼性に関する情報を利用者に通知する方式が有効であると考えられる。本稿では、利用者に通知するDNS回答の信頼度を算出するために必要なチェックの内容とチェック方式について検討した結果を示す。

2. DNS回答の信頼性

現在、ネームサーバが管理しているデータに署名を付けることによって、DNSデータの改竄を検知することが可能なDNSSEC（DNS Security Extensions）[1]が提案されている。DNSSECが導入されれば、DNSの利用者は、署名を検証することで、DNSからの回答がネットワーク上やホスト上で改ざんされていないことを検証することが可能となる。しかし、ネームサーバは様々な組織が運用しているため、すべてのネームサーバにDNSSECが導入されることを期待することは難しい。さらに、ネームサーバのセキュリティレベルが異なるため、どのネームサーバに問い合わせを行うかによって回答の信頼度が異なるという問題がある。

そこで、著者らは、ネームサーバからの回答に対して、データの内容や、ネームサーバの運用管理面に対する評価値を、DNS回答の信頼性情報として利用者に提供し、利用者側でDNS回答の信頼性を判断できる仕組みを提案している[2]。DNS回答の信頼性情報は、図1のように、回答データを保持する回答者マシン（ネームサーバ）に関する信頼度属性S、回答データに関する信頼度属性D、および回答データが要求元に伝わる際の通信路に関する信頼度属性Tの3つに分類しており、本稿では、各信頼度属性を評価するためのチェック内容について検討していく。

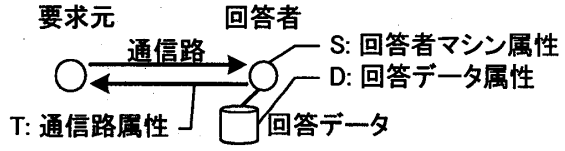

図1 DNS問い合わせにおける信頼度属性

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

3. 信頼度算出のためのチェック基準

DNSの運用に対する要求事項やデータの信頼度については、表1に示すRFC（Request for Comments）に記載されており、この内容を参考にしてチェック項目を抽出することができる。

表1 信頼度チェックの基準となるRFC

RFC 1912	Common DNS Operational and Configuration Errors
RFC 2181	Clarifications to the DNS Specification
RFC 2870	Root Name Server Operational Requirements

RFC 1912 [3]では、DNSのゾーンデータを作成する際に犯しやすい誤りについて述べられている。これらは、主に、回答データに関する信頼度属性Dに関係する。

RFC 2181 [4]の5.4.1節では、回答者がプライマリマスタであるか、セカンダリマスタであるか、データがキャッシュされたものであるか、権威付きであるか、といった観点からDNS回答の信頼度について述べられている。これらも回答データに関する信頼度属性Dに関係する。

RFC 2870 [5]では、ルートネームサーバの運用に関する要求条件について記されており、サーバ自身に求められる機能、物理セキュリティ、ネットワークセキュリティ、認証・プロトコルセキュリティ、運用者間の連絡に関して述べられている。これらは、主に、回答データを保持する回答者マシンに関する信頼度属性Sおよび回答データが要求元に伝わる際の通信路に関する信頼度属性Tに関係する。

4. 信頼度算出のためのチェック項目の抽出

以上のRFCの記述を基に、ネームサーバの安全性および可用性（信頼度属性S）、データの一貫性および原本性（信頼度属性D）、通信路の安全性（信頼度属性T）に関するチェック項目の抽出を行った。なお、このチェック項目は、リモートからDNSプロトコルを使用してチェックできるもののみを対象とし、ネームサーバの物理セキュリティや、運用者間の連絡に関することは対象外とした。

4.1 ネームサーバの安全性チェック（信頼度属性S）

1. 安全で信頼性のあるネームサーバソフトウェアを使用していること（RFC 2870）
2. WKS、HINFO、TXTレコードなどでネームサーバの情報を提供していないこと（RFC 1912）

4.2 ネームサーバの可用性チェック（信頼度属性S）

1. 再帰問い合わせを禁止していること（RFC 2870）
2. セカンダリネームサーバ以外とのゾーン転送を禁止していること（RFC 2870）
3. 同じゾーンを管理するネームサーバが2台以上存在すること（RFC 1912）

4.3 データの一貫性チェック（信頼度属性 D）

1. Lame Delegation になっていないこと（RFC 1912）
2. ネームサーバのホスト名と IP アドレスが、正引きと逆引きで一致すること（RFC 2870）
3. 逆引きした結果が A レコードの内容と一致すること（RFC 1912）
4. 同じ owner に対して、CNAME レコードが別に存在しないこと（RFC 1912）
5. MX、CNAME、PTR、NS の各レコードで指定されているホスト名が別名でないこと（RFC 1912）
6. NS レコードで指定しているネームサーバが別ドメインに属している場合は、そのネームサーバのグルーレコード（A レコード）がゾーンデータ中に存在しないこと（RFC 1912）

4.4 データの原本性チェック（信頼度属性 D）

1. 回答したネームサーバはプライマリマスタか、セカンダリマスタか（RFC 2181）
2. セカンダリマスタの場合は、SOA レコードの Refresh 値が異常に長くないこと（RFC 2181）
3. 回答データは、権威付きのデータか、キャッシュされたデータか（RFC 2181）
4. キャッシュされたデータの場合は、TTL 値が異常に長くないこと（RFC 2181）

4.5 通信路の安全性チェック（信頼度属性 T）

1. 0 以外の正しい UDP チェックサムが付いていること（RFC 1912、RFC 2870）
2. TSIG（Transaction Signatures）[6] などのセキュリティプロトコルを使用して、相手認証とメッセージ認証を行っていること（RFC 2870）

5. 信頼度算出のためのチェック方式

抽出した各チェック項目を基に、DNS 回答の信頼度をチェックする方式を検討した。DNS 回答の信頼度は、DNS の問い合わせ経路と密接に関連することから、ユーザが DNS 問い合わせを行う際に、同時にチェックを行う必要がある。

信頼度算出のためのチェックは、図 2 のように、ローカルネームサーバが行い、各ネームサーバから得た回答に対してチェックを行うだけでなく、信頼度のチェック用に別の問い合わせを発行してチェックを行う。

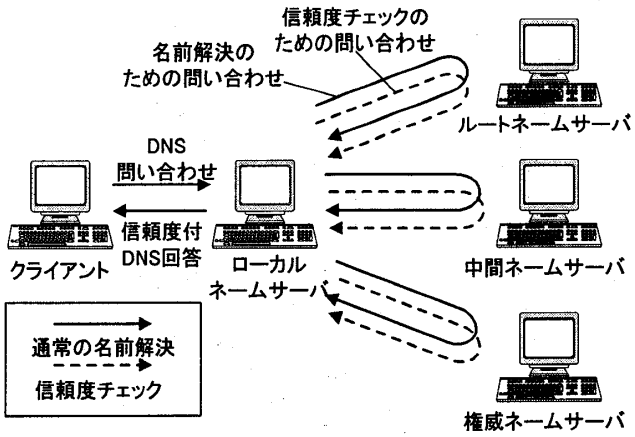

図 2 信頼度チェックの問い合わせ

5.1 ネームサーバから得た回答に対する信頼度チェック

回答パケットの DNS ヘッダ中の RA（Recursion Available）ビットや AA（Authoritative Answer）ビットを確認することで、再帰問い合わせの許可／不許可や、権威の有無をチェックする。また、TSIG などの使用の確認や UDP チェックサムの検証を行う。さらに、回答データの内容を確認し、回答レコードの TTL 値、別名の使用、権威を持つネームサーバの台数などをチェックする。

5.2 問い合わせ先のネームサーバに対する信頼度チェック

各ネームサーバに対しては、通常の問い合わせとは別に、以下の問い合わせを行う。ただし、ゾーン転送や逆引きの問い合わせは、DNS のトラフィックを著しく増加させるため、実際の使用については、さらに検討を行う必要がある。

- ネームサーバプログラムのバージョンの問い合わせ
- ドメイン名をキーとした ANY 問い合わせ（SOA／NS レコードの取得、CNAME レコードの存在チェック）
- 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（CNAME レコードの存在チェック）
- ゾーン転送の問い合わせ
- 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

5.3 最終的な回答を得た後の信頼度チェック

最終的に回答が得られた場合は、さらに以下の問い合わせを行い、回答データの一貫性をチェックする。

- 得られた IP アドレスをキーとした逆引き問い合わせ
- 得られたホスト名をキーとした正引き問い合わせ
- 得られたレコードの owner をキーとした ANY 問い合わせ（CNAME レコードの存在チェック）

6. まとめ

本稿では、DNS 回答の信頼度を算出するためのチェック項目について、RFC の記述を基に具体的に検討し、さらに、名前解決時にリモートからチェックを行う方法について検討した結果を示した。今後は、検討したチェック方式をプロトタイプとして実装し、動作検証を行う予定である。

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] RFC 2535, “Domain Name System Security Extensions”, March 1999.
[2] 渡辺, 山岡, 松田, “DNS における信頼性情報の付与に関する一検討”, 情報処理学会第 64 回全国大会講演論文集(分冊 3), pp.393-394, March 2002.
[3] RFC 1912, “Common DNS Operational and Configuration Errors”, February 1996.
[4] RFC 2181, “Clarifications to the DNS Specification”, July 1997.
[5] RFC 2870, “Root Name Server Operational Requirements”, June 2000.
[6] RFC 2845, “Secret Key Transaction Authentication for DNS (TSIG)”, May 2000.