DNS の信頼性とセキュリティ問題

力武 健次
大阪大学情報科学研究科 /
（株）KDDI 研究所 セキュリティグループ
rikitake@ist.osaka-u.ac.jp / kenji@kddilabs.jp
2003 年 10 月 31 日

概要

DNS（ドメイン名システム）はインターネットの基本サブシステムの 1 つであり，ほとんどすべてのアプリケーションが依存している．しかしそれにもかかわらず，DNS に対する外部からの攻撃に対する防御は十分というには程遠いのが現状である．

本稿では DNS の広義のセキュリティ，つまりシステム全体としての信頼性を高めつつ，個別のなりすましや DoS（サービス拒否攻撃）を防ぐために考慮すべき事項と実際の手法について論じる．

1 はじめに: DNS のしくみ

DNS [1, 2] はドメイン名に対応する IP アドレスやメール配送先の MX (Mail eXchanger) などの情報を関連づけるために不可欠である．Web ブラウザに入力する URL (Uniform Resource Locator) [*1]からアクセスすべき HTTP サーバを確定するには，サーバのドメイン名 [*2]に対応した RR (Resource Record) のうち IPv4 アドレスを示す A RR に対する DNS 参照が必要である．また，DNS が参照できなくなれば，電子メールを配送することはできなくなる．

DNS の実体は複数のサーバが連携した分散データベースである．各々のサーバは各ドメインの階層に対応した RR の集合であるゾーン (Zone) 情報を持ち，ゾーンの上下関係に対応した階層構造を組んでいる [*3]．最上位ゾーンの情報は 13 個あるルートサーバ (Root Servers) が保持しており，そこから下位ゾーンの情報を委任 (delegate) される形で各組織の管理者まで委任関係の階層構造ができるようになっている．

上位ゾーンから下位ゾーンへの委任は具体的には NS RR を設定することで行われる．NS RR によって，特定のゾーンの一部が別のサーバを参照するようになる [*4]．委任のしくみを活用することで，上位ゾーンの管理者は下位ゾーンの管理者が自由に情報設定することを許しつつ，上位ゾーンの情報を改変しないことを保証できる．

DNS はゾーン情報を一定の認証のもとに複製する仕組みを備えている．複製先に NS RR が設定されていればその複製先も公式な (authorized) サーバとなる．一方，頻繁にアクセスする相手の情報に対して，個別に非公式な複製を行うことも慣習として行われている．

2 DNS のセキュリティとは

DNS でのセキュリティを考える際に重要なのは，DNS の持つ情報，具体的には RR の集合は原則として公開情報だということである [*5]．これはインターネットプロトコルの多くが，同一内容の DNS に常にアクセスできているという前提で動いているからである．例えばあるドメイン内のホストをインターネット全域からアクセス可能にするためには，まず DNS サーバをアクセス可能にしなくてはならない．そうしなければドメイン名と IP アドレスの対応関係がつかないからである．

また，基本的には DNS 内の RR は（少なくとも本稿執筆の時点では）ホスト単位の情報であり，それを使う個人の情報までは関知していない．つまり個人単位のプライバシーを DNS で

[*1] たとえば http://www.cmc.osaka-u.ac.jp/SecureNet/ など．

[*2] この場合は www.cmc.osaka-u.ac.jp．

[*3] 多くの場合 1 つのサーバが複数階層のゾーンに対応する情報を持っているため，サーバの階層構造がゾーンの階層構造に 1 対 1 に対応しているわけではない．

[*4] たとえば cmc.osaka-u.ac.jp のゾーン情報を持つサーバは，osaka-u.ac.jp のゾーン情報の中に NS RR として書かれている．

[*5] もちろん組織内限定のプライベートネットワーク内の DNS 情報は組織外に出るべきではないが，これとて組織内に対しては原則公開していると考えるべきである．

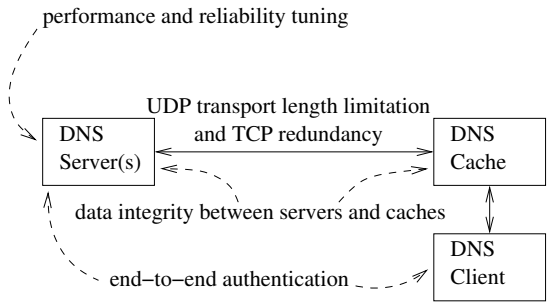

図 1: DNS リゾルバーキャッシューサーバ間の関係

扱うというのは本来適切な運用法ではない [*6].

このような状況下での「DNS のセキュリティ」とは,

DNS 全体の情報の一貫性 複数のサーバ間の委任関係に矛盾がなく，また複製されたゾーン情報がすべて同一であり相違がないこと

RR の認証 RR が適切な管理者によって設定されたことが証明できること

各プログラムとプロトコルの信頼性 DNS のソフトウェア自身にバグがなく動作し，かつ外部からの DoS 攻撃にも耐えられるだけの十分な処理能力を持っていること，またトランスポートなど各層のプロトコルがさまざまな転送要求に対応できること

という観点から考えられるべきである.

3 DNS 全体の情報の一貫性

DNS のクライアントであるリゾルバ (resolver) は，効率良くサーバをアクセスするためにキャッシュ (cache) を使うのが一般的である (図 1)．この際 DNS 全体の情報の一貫性を損なう可能性のある問題を以下に述べる.

TTL とキャッシュ更新の問題 DNS では，各 RR またゾーン単位で設定される TTL(有効期間) による更新の遅れが発生する．DNS は含む機器構成情報は頻繁には変わらないという前提のもとで設計されているため，数分から数時間程度の TTL が各 RR に設定されており，それが終わるまでは情報が旧いままになる．昨今のホスト構成の頻繁な変化に対応した DNS UPDATE [3] 等による情報更新等が普及した場合，この更新の遅れはホスト認証の失敗あるいは間違いにつながる可能性が大きい.

ゾーン情報不一致の問題 また，あるゾーンに対する複数サーバの内容の不一致により，リゾルバやキャッシュが受け取る RR 情報がアクセスする場合ごとに異なる可能性がある．DNS のサーバ情報の更新は Zone Transfer という各ゾーン情報の任意のシリアル番号に依存したサーバ間ファイル転送で行われているのが一般的だが，この方法ではシリアル番号の誤操作や途中回線は何もしない状態では暗号化されないなどの問題がある．これに対してはシリアル番号に依存しない rsync [4] を暗号化シェル OpenSSH [5] を通して実行してゾーン情報を複製し一貫性を高めるなどの対策がある.

DNS 情報の一貫性の問題は，DNS 情報全体の委任関係を子細に辿って検査することが事実上不可能である以上，各管理者の能力に委ねられるところが大きい．現在能力の高いシステム管理者が少ない現状を考えると，これも広義のセキュリティ問題といってよいだろう.

4 RR の認証

DNS は他の多くのアプリケーション同様，暗号化による RR の認証の仕組みを持っていない．このため不正なサーバやキャッシュを通じて虚偽の RR を送り込むことができてしまう．これを利用すれば，MX RR の書換えによる電子メールの横取りや NS RR の書換えによるゾーン/ドメイン全体の乗っ取りができる.

このような状況を防ぐために, DNS サーバーリゾルバ間通信については，DNSSEC [6] という枠組が提案された．DNSSEC では，RR ごとに公開鍵暗号によるデジタル署名を付加して検査を行う方式が提案されている．また, DNS のサーバーリゾルバ間通信では，共通鍵暗号による TSIG [7] や公開鍵暗号による SIG(0) [8] によって，それぞれのサーバーリゾルバ間のやり取りの相手が偽物でないことを保証する方法も

[*6] コンピュータの個人所有の進展が 1 人 1 つ以上のホストという状況を進めているのは事実だが，そのことが各ホストを複数人で共有する可能性を否定するものではない.

提案されている．しかし，DNSSEC や SIG(0) は RR ごとの計算量が多いという問題があり，TSIG では鍵の配布をどうするかという共通鍵暗号特有の問題がある．

しかし実際には DNSSEC やその関連仕様を実装していないサーバやリゾルバも多く，RR の認証を行うのは非常に困難である．また実用化の時点では，認証に使う公開鍵の登録作業が大規模になるため，鍵管理の問題が解決しないことには実用化は難しいといえる．

5 プログラムとプロトコルの信頼性

DNS の土台になるのは, サーバ, キャッシュ, リゾルバといった各プログラム，またそれらの間で通信を行うためのプロトコルである．これらの信頼性を高めることは，DNS 全体の信頼性を高めることにつながる．筆者の現在の研究課題はこの分野を中心にしている．

DNS プログラムとプロトコルの信頼性について考えられなければならないことは無数にあるが，代表的な問題の例を挙げると以下のようになる．

分散 DoS 攻撃　DNS サーバーは基本的に対外公開であり，公衆インターネット全域から狙われることを予想しておかなければならない．DNS データベースの検索応答プロトコルのやり取りのうちほとんどが UDP 上で行われているため，対外的に公開されている UDP ポートを使った単純な同一内容の繰り返しによる DoS 攻撃でも効果を持つ． 2002 年 10 月 21 日に起こったルートサーバへの分散 DoS 攻撃 [9] では，機器構成に非常に大きな余裕を持たせていたため実害はほとんど生じなかったものの，今後のルートサーバ機器の増強計画に影響を与えた．

プログラムの脆弱性攻撃　これも前項同様 DNS サーバーが基本的に対外公開されなければならないことに起因する問題だが，最も普及している DNS ソフトウェアである BIND [10] の場合，サーバーはもちろんのこと，諸 OS の基本機能として実装されているリゾルバにもバグがあり定期的にこれらに関する脆弱性の警告が出ている [11].

トランスポート層のメッセージ長制限

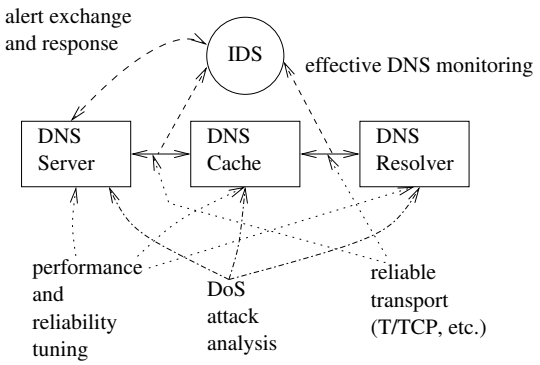

図 2: DNS プログラムとプロトコルの信頼性向上策

RFC1035 Section 4.2.1 では，DNS サーバ－リゾルバ間の一回のやり取りの UDP での長さを 512 バイト以下に制限している．512 バイトを越えた場合は，問合せへの返答は 512 バイトまでに切り詰められてその旨 RR ヘッダにある TC (truncated) ビットが立った返事が返ってくるため，再度 TCP での問合せをしなければならない．
この制限によって，現在ルートサーバの IPv4 アドレス数は 13 に留められている [*7]．また，DNSSEC では，暗号認証の署名記録のためサーバ－リゾルバ間の一回のやり取りのバイト数が増えることにより， TCP で再試行しなければならない事例が増え能率が落ちる可能性が予見されている [12]．同様の現象は，IPv4 から IPv6 への移行の際に，A RR を AAAA RR に換えるまたは両者を併存させることでも起こり得る．

これらの信頼性問題に対する向上策として，現在筆者は以下の事項を研究している（図 2）．

- DNS サーバへ模擬 DoS 攻撃を行い負荷をかけた際の反応を見ることで，サーバの改善点を解析し速度向上のための開発を行っている．現在は OS によるオーバーヘッドが大きいことが判明しており [13]，OS に負荷の大きいコンテキス

[*7] 一例としてルートドメイン `.` に対する SOA RR の問合せを `a.root-servers.net` へ non-recursive query によって行うと，返事として SOA 1 つ，NS 13 個，A 13 個の RR を含む 493 バイトが返ってくる．

ト・スイッチング等の頻度を減らすなどで性能向上ができないかどうかを検討している．

- DNS に関する大規模ネットワークの実トラフィックを収集し内容を解析することで DNS 関連パケットの傾向を割り出し，DNS ソフトウェアを攻撃から守るために使える情報を抽出するための技術開発を行っている．これは IDS（侵入検知システム）的手法の応用でもある．
- DNS サーバ－リゾルバ間のトランスポート層プロトコルについては， UDP で扱えるパケット長を伸ばすための拡張仕様 EDNS0 [14] が提案されている．実際に BIND では最大 4096 バイトまで拡張を許している事例が多い．しかしこの拡張仕様自身が不適切な実装により BIND サーバの停止を引き起こす事例 [15] もあり，必ずしも唯一の解とは言えない側面がある．そこで筆者達は別案の 1 つとして DNS のトランスポートに適した TCP の拡張である T/TCP [16] の実験を行い，その有用性を示した [17].

6 まとめ

本稿では DNS の信頼性とセキュリティ問題に関して，情報の一貫性，RR の認証，そしてプログラムとプロトコルの信頼性の 3 点を主に解説した．

DNS のセキュリティを考えるにあたっては，暗号技術によるプライバシー保護だけではなく，自由にアクセスできるシステムの信頼性向上と脆弱性排除という側面で論じるべきと筆者は考える．

謝辞

本稿執筆にあたり，日頃から研究活動を支援してくださる大阪大学サイバーメディアセンターの下條真司教授と研究室の皆様，また（株）KDDI 研究所の浅見徹所長と同セキュリティグループの皆様に感謝します．

参考文献

[1] Mockapetris, P. V.: Domain names – concepts and facilities (1987). RFC1034 (also STD13).

[2] Mockapetris, P. V.: Domain names – implementation and specification (1987). RFC1035 (also STD13).

[3] Wellington, B.: Secure Domain Name System (DNS) Dynamic Update (2000). RFC3007.

[4] A. Tridgell and P. Mackerras: Rsync. http://rsync.samba.org/.

[5] The OpenBSD Project: OpenSSH. http://www.openssh.org/.

[6] Eastlake, D.: Domain Name System Security Extensions (1999). RFC2535.

[7] Vixie, P., Gudmundsson, O., Eastlake, D. and Wellington, B.: Secure Key Trancsation Authentication for DNS (TSIG) (2000). RFC2845.

[8] Eastlake, D.: DNS Request and Transaction Signatures (SIG(0)s) (2000). RFC2931.

[9] Vixie, P., Sneeringer, G. and Schleifer, M.: Events of 21-Oct-2002. http://f.root-servers.org/october21.txt.

[10] Internet Software Consortium: BIND. http://www.isc.org/bind/.

[11] CERT/CC: Multiple Vulnerabilities in BIND. CERT Advisory CA-2002-31, http://www.cert.org/advisories/CA-2002-31.html.

[12] Gudmundsson, O.: DNSSEC and IPv6 A6 aware server/resolver message size requirements (2001). RFC3226.

[13] Rikitake, K., Sugaya, F., Nakao, K., Nogawa, H. and Shimojo, S.: Resource Consumption Analysis of DNS Servers against DoS attacks, *IPSJ SIG Technical Reports 2003-QAI-8*, Vol. 2003, No. 68, pp. 51–54 (2003).

[14] Vixie, P.: Extension Mechanisms for DNS (EDNS0) (1999). RFC2671.

[15] CERT/CC: Overly large OPT record assertion. CERT Vulnerability Note VU#229595, http://www.kb.cert.org/vuls/id/229595.

[16] Braden, R.: T/TCP – TCP Extensions for Transactions Functional Specification (1994). RFC1644.

[17] Rikitake, K., Nakao, K., Nogawa, H. and Shimojo, S.: T/TCP for DNS: A Performance and Security Analysis, *IPSJ Journal*, Vol. 44, No. 8, pp. 2060–2071 (2003).