Gibson Research の DNS Spoofability Test を用いた フルサービスリゾルバのセキュリティ評価

田中　健吾 [1),2)]

1) 香蘭女子短期大学 情報センター
2) 香蘭女子短期大学 ライフプランニング総合学科

tanaka@koran.ac.jp

Security Evaluation for Full-Service Resolver by Using DNS Spoofability Test of Gibson Research

Kengo Tanaka [1),2)]

1) Information Technology Center, Koran Women's Junior College
2) Department of Comprehensive Studies for Life Planning, Koran Women's Junior College.

概要

Gibson Research は DNS Spoofability Test という、DNS キャッシュポイズニングに対するフルサービスリゾルバの対策状況を評価する Web サービスを公開している。その DNS Spoofability Test を用いて、4 つのフルサービスリゾルバの安全性評価を行った。4 つの内、2 つは Google Public DNS と Open DNS と呼ばれるオープンリゾルバであり、残り 2 つは商業プロバイダーのものである。評価内容の中心は、通信に使用するポート番号とトランザクション ID のランダム化である。本稿では、4 つのフルサービスリゾルバの評価結果について解釈と考察を行った。その際、DNS Spoofability Test のサイトに記述されている安全性の評価項目についての説明を紹介すると共に、著者による平易な解説も加えた。

1　はじめに

著者が勤務する短期大学では、これまで、契約関係のある商業プロバイダーのフルサービスリゾルバを用いることで、名前解決を安定稼働させる選択をしてきた。

2016 年度に SINET5 へ接続する工事を行った。その際、SINET5 にはフルサービスリゾルバを提供するサービスが不在であったため、本学が契約している商業プロバイダー（以下、プロバイダーA）のフルサービスリゾルバを、学内 LAN 上の DNS サーバのフォワーダーとして利用することを試みた。しかし、オープンリゾルバでないために、SINET5 側の回線からは参照できなかった。そのために、SINET5 を通じてインターネット接続する場合でも、名前解決だけは、プロバイダーA を利用するように静的経路情報を設定することで対応した。

上記の構成で、SINET5 を通じたインターネット接続が稼働するには、プロバイダーA への接続に障害がないことが前提となり、2 回線で冗長化構成するメリットが享受できていない。

この問題の解決方法として、プロバイダーA の障害時には、緊急措置としてオープンリゾルバを一時的に利用することを検討した。有名なオープンリゾルバとして、Google Public DNS（以下、Google DNS）や Open DNS などが知られているが、どのオープンリゾルバを利用するかを結論するには、その安全性や応答性能を評価する必要があった。その際に用いたのが、Gibson Research 社の DNS Spoofability Test（以下、Spoofability Test） [1] と DNS Benchmark [2] である。応答性能は DNS Benchmark を用いることで、フルサービスリゾルバの名前解決時間を計測することができる。DNS Benchmark については、文献[3]で説明しているので、そちらに譲りたい。他方、安全性については、Spoofability Test を用いることで、

DNS キャッシュポイズニング対策として推奨されているポート番号とトランザクション ID（以下、TXID）のランダム化を、可視化するなどして評価することができる。

本稿の目的は二つある。一つは、実際に Spoofability Test を用いて、オープンリゾルバを含めた 4 つのフルサービスリゾルバを評価した結果と、その解釈について述べることである。Spoofability Test のサイトには、カミンスキー攻撃発見時の初期対応に関するエピソードの紹介にはじまり、その対策方法や攻撃に対する安全性の評価方法などについて英文の解説が掲載されている[1]。本稿のもう一つの目的は、攻撃に対する安全性の評価方法および評価結果の解釈の部分について、日本語で、さらに平易な解説を加えて紹介することである。

2 DNS キャッシュポイズニング

DNS キャッシュポイズニングの典型的な攻撃方法の一つは、攻撃者が何らかの方法で、正当な権威サーバからの応答がフルサービスリゾルバへ届く前に、偽の名前解決情報をフルサービスリゾルバへキャッシュさせることである。その結果、そのフルサービスリゾルバで名前解決を行うユーザをフィッシングサイトなどの成りすましサイトへ誘導したり、メールを不正に取得したりすることが可能となる。この節では、DNS プロトコルの脆弱性とカミンスキー攻撃への典型的な対策方法について述べる。

2.1 DNS プロトコルの脆弱性

DNS プロトコルは主に UDP を使用しており、クエリには送信元の IP アドレスやポート番号、TXID、他が含まれる。権威サーバからの応答は、TXID とポート番号が一致すると、正しい応答としてフルサービスリゾルバへキャッシュされる。TXID は 16bit であるので、攻撃者はすべての ID を持つ詐称応答を作り出し、フルサービスリゾルバへ送信し続けることは容易に実現可能であり、権威サーバからの応答よりも早くキャッシュされればポイズニング成功となる。しかし、「フルサービスリゾルバへ大量の詐称応答を送るので異常検出されやすい」「詐称応答より先に正しい応答がキャッシュされてしまえば TTL 値の設定時間が経過するまでは再攻撃できない」という理由で、カミンスキー攻撃の発見以前は現実には起こり得ないと考えられていた。

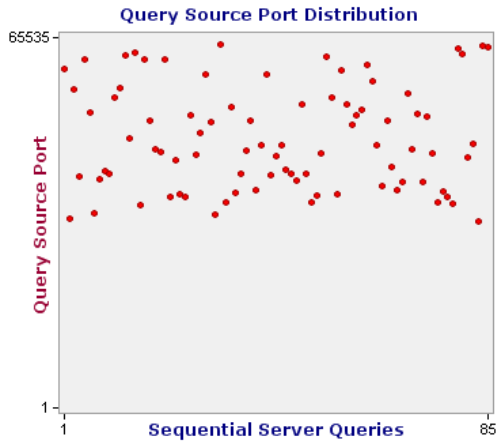
2.2 カミンスキー攻撃と推奨されている対策方法

カミンスキー攻撃は、TTL 値の間、再攻撃できないという問題を、「IP アドレスを詐称したいドメイン名の偽権威サーバを準備する」「攻撃対象となるフルサービスリゾルバのドメイン名に現実には存在しないランダムなサブドメイン名を加えたドメイン名の問い合わせを、連続して行う」という二つを組み合わせることで解決した。サブドメイン部分が存在しないランダムな文字列であることより、フルサービスリゾルバは毎回、権威サーバへ問い合わせを行うことになる。権威サーバからの応答よりも早く、攻撃者が Authority Section に IP アドレスを詐称したいドメイン名の権威サーバを、予め構築しておいた偽権威サーバにゾーン分割する NS レコードをキャッシュできれば、第一段階のポイズニング成功である。その後、クライアントがフルサービスリゾルバへ詐称したいドメイン名を問い合わせると、偽権威サーバから誘導先の偽 IP アドレスがフルサービスリゾルバへキャッシュされ、ポイズニングが完成となる。

カミンスキー攻撃対策で最も推奨されているのが、ポート番号のランダム化である。TXID の 16bit に加えて、UDP のポート番号も 16bit であり、このエントロピーを最大限に利用すると、ポート番号が固定されている場合よりも攻撃成功の可能性を 65536 分の 1 に軽減できる。

3 DNS Spoofability Test

Spoofability Test のサイト[1]の下部にある「Initiate Standard DNS Spoofability Test」というボタンをクリックするだけで、端末に設定している DNS サーバが参照可能なフルサービスリゾルバを検索して、安全性評価を行うこと



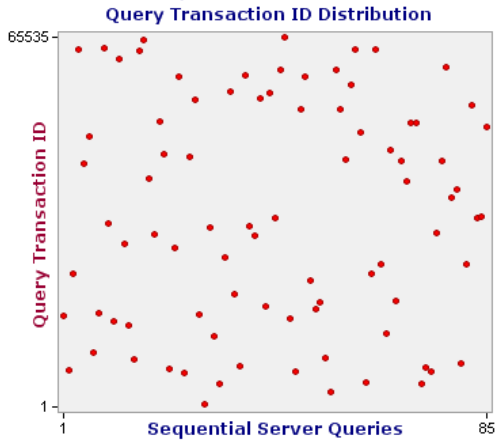
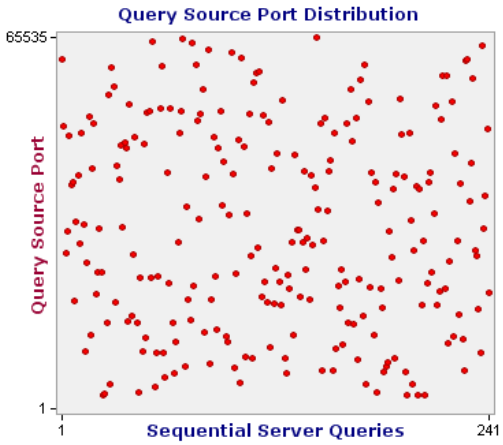


図 1　Google Public DNS



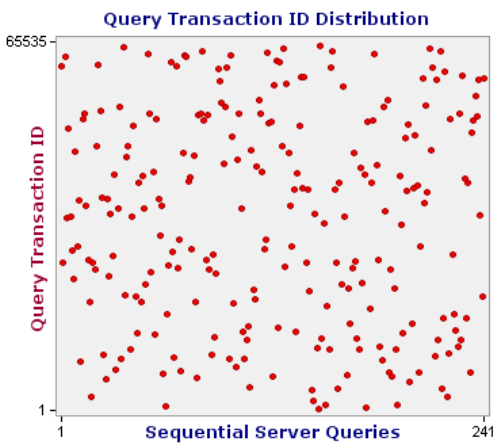
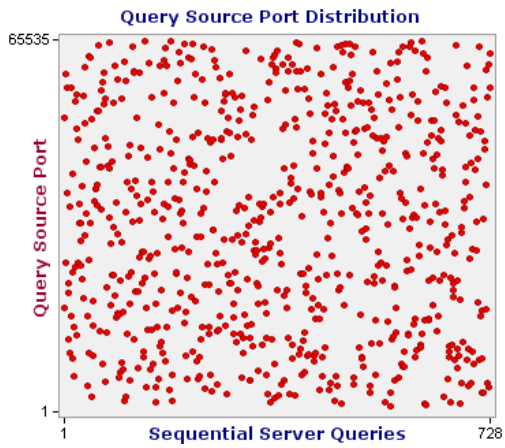


図 2　Open DNS



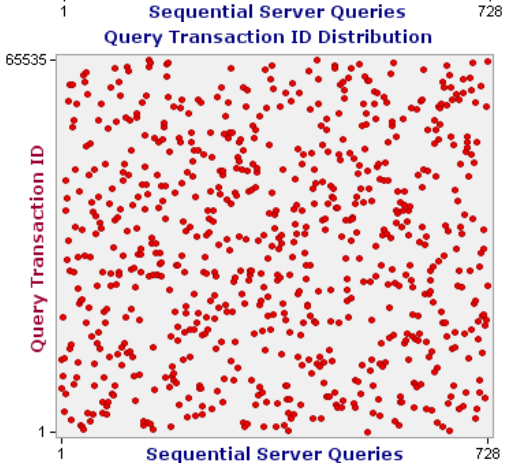
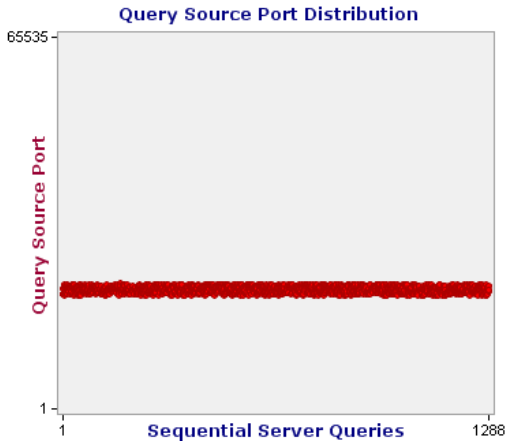


図 3　プロバイダーA



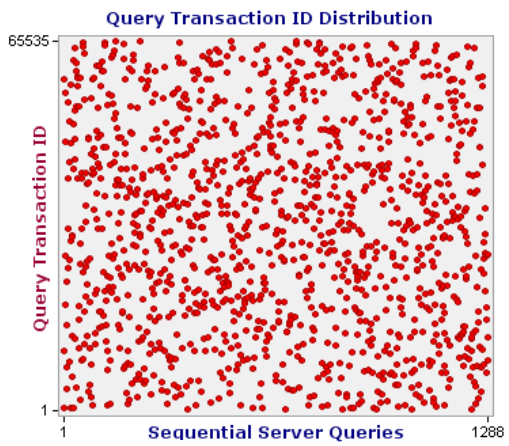


図 4　プロバイダーB

ができる。結果は、「Scatter Charts」「Bit Predictability Charts」「Analysis Tables」「Access Details Table」の 4 項目で表示される。テストの概要は、参照可能なフルサービスリゾルバが、Gibson Research 社が準備した本テスト用のドメインの権威サーバに連続してクエリを投げることで、使用するポート番号と TXID を記録するというものである。

この節では、オープンリゾルバである Google DNS（8.8.8.8）と Open DNS（208.67.222.222）に加えて、本学が契約している商業プロバイダーA と、著者が自宅で契約している商業プロバイダー（以下、プロバイダーB）のフルサービスリゾルバのテスト結果を示すと共に、その解釈について述べたい。

尚、プロバイダーA 以外は、端末に設定したフルサービスリゾルバの先に、更にフォワーダーとなるフルサービスリゾルバが複数存在する。それぞれ、フォワーダー中の一つの結果だけを図示するに留めるが、基本的には複数あるフォワーダーはいずれも同じ傾向を示していた。

3.1 Scatter Charts

それぞれのフルサービスリゾルバのテスト結果を図 1～4 に示す。いずれの図も、横軸が投げたクエリの個数になっている。また、各番号の上の図の縦軸がポート番号、下の図の縦軸が TXID になっている。いずれも、16bit であり、10 進数での値は 0～65535 となる。同サイトには、以下と同趣旨の解説が述べられている。

・各散布図内の次の点を上手く予想できる攻撃者は、詐称されているが、正常に機能する応答を作成することで、ネームサーバのキャッシュを害することができる。

・クエリのポート番号と TXID を予想される可能性を小さくするためには、両者のすべての番号の範囲（0～65535）を使用すべきである。限られた範囲の番号しか使用しないと、攻撃者に予測されやすくなる。つまり、散布図に大きく空いた場所があれば、良く無い状態である。

上記の解説で警告されている状況に該当する

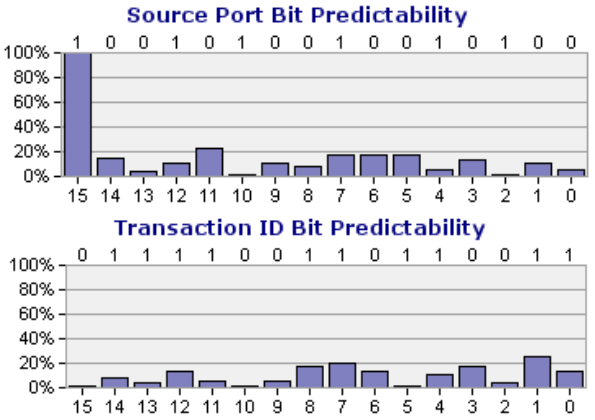


図 5　Google Public DNS

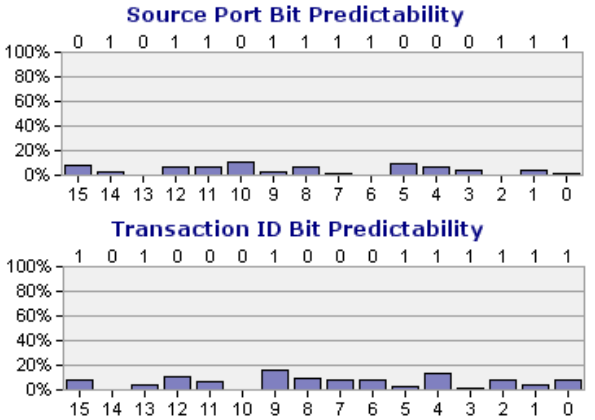


図 6　Open DNS

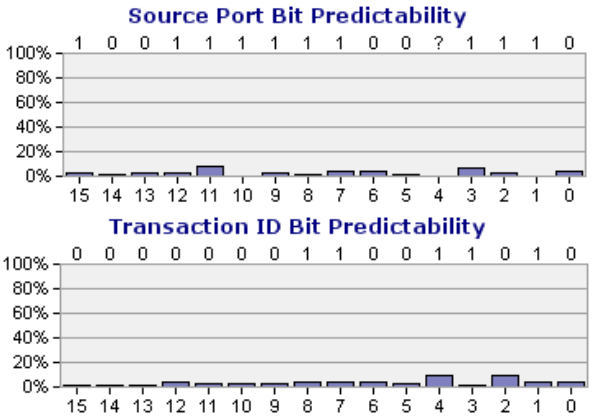


図 7　プロバイダーA

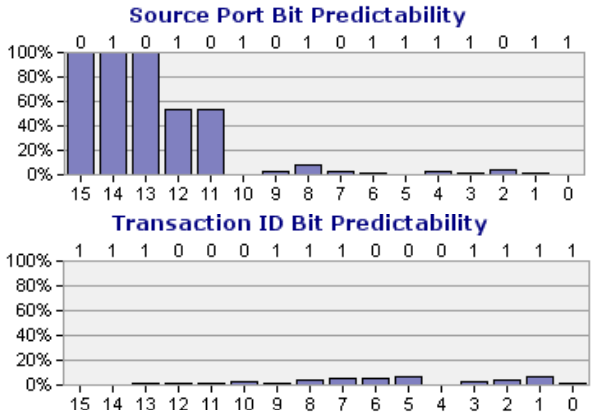


図 8　プロバイダーB

のは、図 1 と 4 のポート番号の方である。図 1 のポート番号は散布図中の上半分に集中して分布していることが分かる。また、図 4 のポート番号はかなり狭い範囲の値しか使用されていないことが分かる。

3.2 Bit Predictability Charts

図 5～8 では、ポート番号と TXID の各桁（0～15）が 0 もしくは 1 のどちらが、どの程度の割合で多く利用されているのかを示した棒グラフである。例えば、横軸が 15 の位置の棒グラフの上部に数字の 1 が記載されていたとする。その棒グラフの縦軸のメモリが、0%では、0 と 1 が同じ割合で使用されており、100%であれば 1 しか使用されていないことになる。

この Bit Predictably 図について、同サイトには、以下と同趣旨の解説が述べられている。

・散布図では一見、ランダムに見える値でも、例えば、4 の倍数になっている可能性もある。この場合、攻撃者は全てのポート番号を推測せずに、4 の倍数だけを対象にすればよいことになる。4 で割り切れるポート番号の場合、Bit Predictably 図では、最下位 2bit が常にゼロになり、16bit の内、2bit は完全に予測可能になる。Bit Predictably 図では、見逃しそうな数字の傾向を見つけるために、ポート番号と TXID に使用される 16bit それぞれの予測される可能性を分析し、表示する。

実際に、図 5 と 8 のポート番号では、上記の解説にあるような、数字の法則性が次のように見て取れる。　図 5 のポート番号においては、最上位 1bit が 1 しか使用されていない。その傾向は図 1 のポート番号の散布図でも、上部にしか点が分布しておらず、2^{15}=32768 より大きい数字しか利用されていないことが明確に分かる。また、図 8 のポート番号では、最上位 3bit が 010 で固定されていることが分かる。その傾向は、図 4 のポート番号の散布図にも明確に出ている。下位 13bit は使用されている様であるので、2^{14}=16384～24575 の範囲の値が用いられていることが推測され、散布図でも実際にその付近に分布が集中していることが明確に分かる。

上記 2 つの傾向は複数回テストを繰り返しても全く同じ結果になるので、使用するポート番号が限定されていると言ってよい。

3.3 Analysis Tables

図 9～12 では、ポート番号と TXID のランダム性に関する判定を以下の 4 項目について行った結果である。4 項目について、同サイトには以下と同趣旨の解説が述べられている。

・Max Entropy

記録された（ポート番号と TXID）の最小値と最大値の間の全ての値を表現するために必要なバイナリービットの数を表している。記録された値の範囲を対数で表現したものであり、16 が最大値で、数が大きいほど良好である。

・Lost Entropy

上記で記録された最小値と最大値の範囲による最大潜在エントロピーが存在し得るにもかかわらず、多数の重複した値は潜在エントロピーを浪費する効果と、詐称応答を可能にする推測を成功させやすくする効果がある。つまり、損失エントロピーは、重複した値が記録されたことで損失したエントロピーの有効ビット数を測定したものである。

・Dir Bias（Direction Bias）

直線的に増加していく値は、良好で大きな最大エントロピー（ポート番号全体の範囲を使用）と、良好なゼロの損失エントロピー（重複番号なし）を有し、これらの基準では非常に優れていることになる。しかし、単純な直線的増加をする値は、明らかに非ランダムであり、すぐに推測できる。つまり、「Direction Bias」測定は、値の傾向における全体のバイアスを検出するために、隣接する値のすべてのペアを検証する。

・Stuck Bits

固定されて変化しない bit 値以上に、値のランダム性を低減させるものはない。すべてのこの様な固定 bit 値は取り得る値の数を半分にし、推測で詐称応答を可能にする効率を 2 倍にする。また、特に下位の方の bit 値は散布図では視覚

的に明確ではない。この測定は固定 bit 値を明確にする。

同サイトの上記 4 項目の解説について、以下、補足と、テスト結果について考察を行いたい。

・Max Entropy

16bit のエントロピーは、$\log_2 2^{16}=16$ となる。最大エントロピーの評価は実際に記録されたポート番号と TXID の最小値と最大値の範囲で測定している。つまり、0 と 65535 の両方が記録されなければ、最大値の 16 にはならない。

テスト結果について、まず、図 1 と 4 のポート番号の散布図を除いた、その他の 6 つの散布図について述べたい。いずれも全体に点が分散しており、それらに固定 bit 値が無いことは図 5～8 でも確認されている。必然的にエントロピーも大きくなる傾向にあり、最大値の 16 に近い値が期待される。実際、図 9～12 の通り、Max Entropy の計測値はいずれも 15.9 以上を示しており、評価は全て「Excellent」となっている。

他方、図 1 のポート番号の散布図は上半分に点が局在していた。図 5 に示されている通り、最上位 bit が固定であり、1 桁分のエントロピーの減少が期待される。実際、図 9 には、14.94 というほぼ理論通りの値が測定結果として示されており、評価結果は「Excellent」より低い「Good」となっている。また、図 4 のポート番号の散布図では、点が帯状に局在した分布であった。ポート番号は図 8 に示されている通り、上位 3bit が固定であり、3 桁分のエントロピーの減少が期待される。しかし、図 12 にはそれよりも低い、11 という値が測定結果として示されており、評価も「Moderate」となっている。

・Lost Entropy

最大潜在エントロピーという言葉が使用されているが、これは、上述したように最大エントロピーを、記録された最小値と最大値の範囲で評価していることより、潜在という言葉が使用されていると推測される。つまり、最小値と最大値の中間の値は本当に使用されているかどうかは、不明ということである。また、重複すればするほど、エントロピーを活かしておらず、重複した数を bit 数に変換したものが、損失エントロピーとなる。

Query Source Port Analysis (worst case)

Max Entropy: 14.94	Good	Dir Bias: 4.76%	Excellent
Lost Entropy: 0	Excellent	Stuck Bits: 1	Moderate

Query Transaction ID Analysis (worst case)

Max Entropy: 15.99	Excellent	Dir Bias: 0%	Excellent
Lost Entropy: 0	Excellent	Stuck Bits: 0	Excellent

図 9　Google Public DNS

Query Source Port Analysis (worst case)

Max Entropy: 15.95	Excellent	Dir Bias: 5%	Excellent
Lost Entropy: 0.01	Excellent	Stuck Bits: 0	Excellent

Query Transaction ID Analysis (worst case)

Max Entropy: 15.98	Excellent	Dir Bias: 7.5%	Excellent
Lost Entropy: 0	Excellent	Stuck Bits: 0	Excellent

図 10　Open DNS

Query Source Port Analysis (worst case)

Max Entropy: 15.97	Excellent	Dir Bias: 2.89%	Excellent
Lost Entropy: 0.01	Excellent	Stuck Bits: 0	Excellent

Query Transaction ID Analysis (worst case)

Max Entropy: 16	Excellent	Dir Bias: 4.26%	Excellent
Lost Entropy: 0.01	Excellent	Stuck Bits: 0	Excellent

図 11　プロバイダーA

Query Source Port Analysis (worst case)

Max Entropy: 11	Moderate	Dir Bias: 3.19%	Excellent
Lost Entropy: 0.42	Moderate	Stuck Bits: 3	Bad

Query Transaction ID Analysis (worst case)

Max Entropy: 16	Excellent	Dir Bias: 0.7%	Excellent
Lost Entropy: 0.02	Excellent	Stuck Bits: 0	Excellent

図 12　プロバイダーB

実際のテスト結果では、図 12 に示されている通り、プロバイダーB のポート番号の損失エントロピーが、唯一、0.41 という大きな値を示している。このことは、ポート番号が上位 3bit 固定であり、狭い範囲のポート番号しか利用できない上に、図 4 にある通り、1288 回というクエリをその狭い範囲で実行したために、番号が重複しやすい傾向になることは必然の結果といえよう。実際、図 4 は、ポート番号が大いに重なっているイメージを支持する描画となっている。

・Dir Bias

クエリを投げるごとに使用する値を、一定の数値間隔で採用するなど、ある法則性に従っているとすれば、その値は攻撃者に推測されやす

くなる。これは、エントロピーの大きさでは測定できない弱点である。図 9～12 に示されている通り、その様な直線的に増加する値の使用についての傾向は無く、評価もすべて「Excellent」となっている。

・Stuck bits

Stuck bits の評価は、図 5～8 の ID Predictably の結果と完全に一致している。Google DNS とプロバイダーB のポート番号は、それぞれ、上位 1bit と上位 3bit が固定であり、図 1 と 4 の散布図ではその影響が明確に分かるが、これが下位 bit であれば、10 進数スケールの散布図では影響が分かりにくい。

3.4 DNS Nameserver Access Details

図 13～16 では、ポート番号と TXID のランダム化以外の安全性を、次の 4 項目に関して、評価した結果である。同サイトには、4 項目に関して、以下と同趣旨の解説が記述されている

・External Ping

外部からの Ping（プロバイダーのローカルネットワークの外部からの ping）に応答しない、特に、DNS サーバが外部からのクエリを無視する場合、機器の存在が幾分、分かりにくくなる。

・External Query

プロバイダーのクライアントに代わって DNS クエリのみを解決する DNS リゾルバは、プロバイダーのネットワーク外のインターネットからのクエリ解決を無視する限り、不可能ではないが、かなり詐称することが困難になるだろう。プロバイダーのリゾルバが外部からのクエリを無視すれば、心配無用である。

・DNSSEC Security

現代的な DNS サーバは先進的で、次世代の技術として知られている「DNS Security」（DNSSEC）をサポートしている。このシステムは、まだインターネット上に広く配備されていないため、DNSSEC をサポートしていることは、ネームサーバが詐称耐性を有していることを意味するわけではない。しかし、サポートしていれば、あなたのプロバイダーがネームサーバを最新の状態を維持しているという良好なサインとなる。

・Alphabetic Case

DNS はアルファベットの大文字小文字に反応しないので、「WWW.GRC.COM」というドメインは「www.grc.com」と同一になる。DNS は無視するように設計されているが、クエリと応答において、アルファベットの大文字小文字を保持する。これは、DNS リゾルバに追加の新たなエントロピーとなる bit を、問い合わせられたドメイン名のアルファベットの文字列を大文字小文字でランダムに変化させることで、付加する機会を与えている。大文字小文字が入り混じったクエリを受けて、それに応答する正当なネームサーバだけが、その応答において、適切な大文字小文字の並びを知ることができる。なりすましサーバは知ることはできない。この方法は、賢明なリゾルバに詐称応答を拒否する別の方法を与えている。私たちは、この様な方法で、意図的に大文字小文字を混在させているサーバが存在しないことを知っているが、このテストを通じて、あなたの関心を集めることを促している。

・Extra Anti-Spoofing

ネームサーバの中には、とりわけ「Nominum」のように先端的で独自性のある詐称対策を採用し

DNS Nameserver Access Details

External Ping:	replied	(It might be better for the server to be less visible.)
External Query:	ignored	(This means the nameserver is more spoof resistant.)
DNSSEC Security:	supported	(This server supports improved security standards.)
Alphabetic Case:	all lower	(An improvement could be created by mixing case.)
Extra Anti-Spoofing:	unknown	(Unable to obtain server fingerprint.)

図 13　Google Public DNS

DNS Nameserver Access Details

External Ping:	replied	(It might be better for the server to be less visible.)
External Query:	ignored	(This means the nameserver is more spoof resistant.)
DNSSEC Security:	absent	(This nameserver might need to be updated.)
Alphabetic Case:	all lower	(An improvement could be created by mixing case.)
Extra Anti-Spoofing:	unknown	(Unable to obtain server fingerprint.)

図 14　Open DNS

DNS Nameserver Access Details

External Ping:	replied	(It might be better for the server to be less visible.)
External Query:	rejected	(It would be better for it to ignore external queries.)
DNSSEC Security:	supported	(This server supports improved security standards.)
Alphabetic Case:	all lower	(An improvement could be created by mixing case.)
Extra Anti-Spoofing:	not present	(No additional anti-spoofing technology.)

図 15　プロバイダーA

DNS Nameserver Access Details

External Ping:	replied	(It might be better for the server to be less visible.)
External Query:	ignored	(This means the nameserver is more spoof resistant.)
DNSSEC Security:	absent	(This nameserver might need to be updated.)
Alphabetic Case:	all lower	(An improvement could be created by mixing case.)
Extra Anti-Spoofing:	unknown	(Unable to obtain server fingerprint.)

図 16　プロバイダーB

ているものがあるため、このテストでは、クエリリゾルバのその他の特性のいくつかが警告の原因になり得たとしても、詐称免疫性があるか否かことを特定するために、各々のクエリリゾルバの製造形式やモデル、バージョンを決定することを試みる。

以下、上記 4 項目に関して、それぞれテスト結果を解釈すると共に、若干の解悦を加えたい。

外部からの ping（External Ping）に関する評価項目は、4 つのフルサービスリゾルバ共に応答する結果である。

外部からのクエリ（External Query）に関しての評価項目は、プロバイダーA は「rejected」となっており、実際、1 で述べたように、プロバイダーA に属していない IP アドレスからは、参照不能であった。他の 3 つは「ignored」という結果になっているが、Google DNS と Open DNS はオープンリゾルバであり、本学固有の PI アドレスからも参照可能であることは確認済みであるので、「ignored」が無視する（応答しない）という意味であれば、矛盾していることになる。また、プロバイダーB も外部からは参照不能であることを確認している。

DNSSEC は権威サーバの応答が、その出自と改変が無いことを、公開鍵暗号方式を採用することで保証されるが、フルサービスリゾルバも DNSSEC に要対応である。テスト結果では、Google DNS とプロバイダーA が対応しており、他の 2 つは非対応であることが示されている。

アルファベットの大文字小文字（Alphabetic Case）の評価項目については、ドメイン名のアルファベットをそれぞれ、大文字小文字へとランダムに変換してクエリを投げることでエントロピーを増大させるという、新しいアイデアを広めることを意図したものである。大文字小文字の 2 通りが 1bit に対応する。例えば、www.grc.com であれば、アルファベット 8 文字であるので、8bit のエントロピーを付加したことになる。テスト結果はいずれも、小文字（all lower）に統一されていることを示している。

追加の詐称対策（Extra Anti-Spoofing）については、例として Nominum が紹介されている[4]。テスト結果は、プロバイダーA だけが、「存在しない」であり、あとは「不明」である。プロバイダーA は Nominum を採用していないことが確認できており、テスト結果と無矛盾である。

4. テスト結果の考察と結論

Spoofability Test には、安全性評価の総評が示される。Open DNS とプロバイダーA は「Excellent」、Google DNS は「Moderate」、プロバイダーB は「Bad」という結果であった。

ポート番号と TXID のランダム化については、図 1～4 の散布図、図 5～8 の Bit Predictably 図、そして、図 9～12 の Max Entropy および Stuck Bits の結果は全て一貫していた。また、同テストが各クエリで用いているポート番号と TXID の値は全て記録されており、実際に同サイトで確認することができる。以上より、これらの評価結果は信頼できると思われる。

他方、ランダム化以外の評価としては、図 13～16 のテスト結果が挙げられる。3.4 で述べた通りであるが、External Query の評価結果を「ignored」の字義通り解釈すると、実際の仕様と異なり、疑問の残る結果となった。

本学で緊急時に利用するオープンリゾルバを Open DNS に結論した。以上の考察に加え、「クエリに対する複数のフォワーダーからの応答の合計が、常に Open DNS の方が 10 倍以上多い」「Google DNS をフォワーダーに設定すると名前解決が遅延する」という点が判断基準である。

参考文献

[1] https://www.grc.com/dns/dns.htm
[2] https://www.grc.com/dns/benchmark.htm
[3] 田中健吾、香蘭女子短期大学における SINE5 への接続と名前解決の構成方法、大学 ICT 推進協議会 2017 年度年次大会、2017 年.
[4] https://www.nominum.com/