香蘭女子短期大学における SINET5 への接続と名前解決の構成方法

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

Connection to SINET5 and How to Configure Name Resolution in the Case of Koran Women's Junior College

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

2016 年度に香蘭女子短期大学では、主として帯域不足改善を目的として、従前のインターネット接続を SINET5 への接続へと移行する工事を行った。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に、名前解決をするシステム構成に関して、通常時は静的経路情報を設定することで、商業プロバイダーのフルサービスリゾルバを、緊急時には、一時的にオープンリゾルバを利用することを採用したり、DNS リレーを導入したりするなどして、いくつかの工夫を行った。また、同時にファイヤーウォール機能や回線の負荷分散機能、冗長化機能の更新も行った。本稿では、これらの工事がおおむね完了した 2017 年 1 月末時点での本学のインターネット接続環境について、大幅なコスト削減と帯域幅の増強、セキュリティ向上を達成することができたので、これらの工事の経緯と結果について報告する。

1　はじめに

著者は福岡市にある 4 学科、1 専攻科を設置している短期大学に勤務している。学生数は 2017 年度現在で約 850 名、教職員数は約 70 名であり、学内の端末台数は教育用・業務用を合わせると約 400 台である。学内のネットワーク基盤やセキュリティ対策、パソコン教室、他、の管理・運営を情報センターが行っているが、所属学科と兼任のスタッフ 2 名で業務を担当しており、専任のスタッフは不在である。情報センターと学内各部署（事務局各部署、各研究室、他）との間で、情報環境基盤および情報機器に関する責任分界点は定めているものの、管轄外の端末や情報システム関連のことにも、しばしば対応したり、相談を受けたりしているという状況である。このような実情から、業務の効率化、サービスの安定稼働、コスト削減、トラブル対策、地方の小規模大学・短大としての標準的なサービスの提供などが、常に中心的課題である。

本稿では、上記の課題の中で、「サービスの安定稼働」に関して、インターネット接続の帯域不足という問題が生じた。帯域不足を解消するために、本学情報センターが 2016 年度に行ったインターネット接続環境やネットワーク機器の更新業務に関して述べたい。

本学では、前期に情報処理入門や情報リテラシーといった、情報処理の入門科目がクラス単位で開講されている。時間割編成上の都合から、同時間帯に複数のパソコン教室で同じ科目を並列して開講している場合が多い。そのような事情から、多数の端末の同時アクセスによる負荷が最大になるのが、前期の同科目が開講されている時間帯となる。2016 年度の、やはり前期に、インターネット接続が遅いといった報告が、学内各所から情報センターへ報告されたことを契機に、インターネット接続環境を見直す必要性

を感じて、回線からルーター、ロードバランサー、他、を 2016 年度に更新する工事を行った。また、その際、運用上で検討を重ねる必要が生じた名前解決の方法とその経緯についても併せて報告したい。

2 インターネット接続環境の更新

2016 年度に更新を行う以前のインターネット接続環境は、5Mbps の帯域保証型の専用線と、100Mbps のベストエフォート型回線をロードバランサーで束ねることで、負荷分散および冗長化構成をとっていた。ロードバランサーのスループットの最大値が 50Mbps であったので、これが、当時の理論上の最大値であった。この構成で、本学のインターネット接続は約 8 年間、運用されてきたが、上述の通り、2016 年度前期に帯域不足が生じた。この節では、2016 年度の 5 月末から計画を立案し、年末から年度末にかけてインターネット接続環境の更新する工事を行ったので、その経緯と詳細について述べたい。

2.1 更新時の検討事項

更新時の検討事項は以下の通りであった。

① 十分な帯域の改善と回線の選択
② 高額な帯域保証型の専用線の存続・廃止
③ ロードバランサー機能の維持
④ ファイヤーウォールの導入
⑤ 回線以外の年間固定費を極力増やさないこと

①②については、これまでの経緯として、次のような事情がある。インターネット接続回線は、物理的断線や機械的な障害などを考慮して、別配線ルートの 2 回線を確保するために、異なる 2 系統の回線を 1 回線ずつ契約することが望ましいと考えられる。

実際に、2016 年 11 月に起こった博多駅前の陥没事故では、多くの断線が生じた。また、年々増加傾向にある台風上陸などの被害による断線も十分に起こり得る。本学近郊には、NTT 系の回線と九州電力系の回線が存在しているが、立地上の都合から、1 系統からしか回線を引くことができていなかった。そのために、これまで、保守契約がある高額な専用線を維持してきた。

帯域を大幅に改善しつつ、専用線の保守契約を維持しながらコストを抑えることを検討した結果、既存の 5Mbps 専用線と 100Mbps ベストエフォート型回線を提供しているプロバイダー兼回線提供業者（以下、旧プロバイダー業者）の契約を廃止して、SINET5 の福岡 DC2 へ接続する専用線と、商業プロバイダーのバックボーンへ 10Mbps で接続する帯域保証型専用線を、新規のプロバイダー兼回線提供業者（以下、新プロバイダー業者）の契約へと移行することを計画した。

本学と福岡 DC2 を理論値上では 1Gbps の帯域幅で接続していることになり、十分な通信速度の改善が見込める。また、新たに契約した 2 回線の月学費は、従来の 2 回線と比較すると、約 40%のコスト削減となり、十分に要件を満たすことが期待できる構成となった。

③④についても以下の通りである。これまで、ロードバランサーで 2 回線を冗長化すると共に、パケットフィルタリングを行うことで、ファイヤーウォールの機能を実装していた。

現状使用していたロードバランサーと同機種で、高いスループットを実現できる上位機種を検討したが、高額であった。その高額な初期導入費や年間固定費をロードバランサーに充てることを考えると、回線冗長化の機能を捨てて、IPS（Intrusion Prevention System：不正侵入防御システム）や WAF（Web Application Firewall）の機能を持ったファイヤーウォールを導入した方が望ましいように思えた。

しかし、IPS や WAF などのいわゆる UTM（Unified Threat Management：統合脅威管理）の機能を使用するには、高額な年間ライセンス料が固定費として必要になるために、標準的なファイヤーウォールの導入も採用しなかった。結果的に、富士ゼロックス社の beat/active を以下の理由より、試験的に利用開始をしてみ

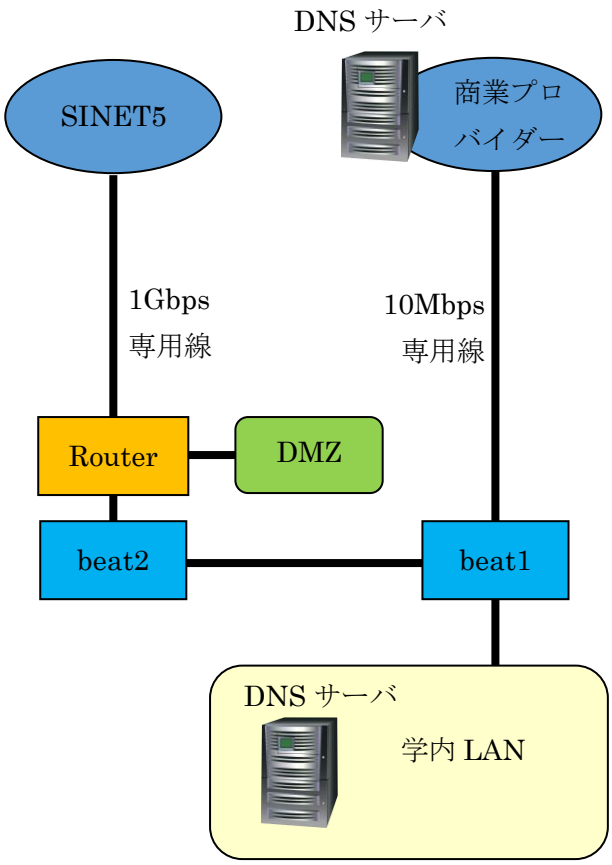

図 1　更新後のインターネット接続環境

るという結論に至った。

一つ目の理由は、簡易的なロードバランサーと IPS の機能を備えているという点である。もちろん、専用機のロードバランサーやファイヤーウォールほどの高機能さや詳細な制御機能は無く、これまで採用していた機種の機能を再現できていない部分もあるが、ルーターと併用することで、最低限、本学のネットワークを構成できる機能を備えていた。また、1Gbps のスループットを実現できるという点から、SINET5 へ接続する専用線の帯域に見合ったパフォーマンスも有していた。

もう一つの理由は、初期導入費が安いことと、専用機の価格とそのライセンス費に比べると、安価な月学費を支払うことで利用開始ができた点である。利用してみて、機能や性能不足が分かった時点で解約すればよいと考えていた。

以上で述べた①～④の更新案で⑤の回線以外の年間固定費についても、ほぼ増やさずに済む理想的なプランを立案することができた。

2.2 更新結果

更新後のインターネット接続環境は図 1 の通りである。学内 LAN 上にある DNS サーバには、商業プロバイダーのバックボーン上にあるフルサービスリゾルバをフォワーダーとして登録している。

図 2 および 3 には、SINET5 側の出口に設置しているルーターのデータ転送速度の計測機能を使用して、1 日間および 1 ヶ月間のデータを記録したものである。図中の横軸は時間軸、縦軸はデータの転送速度である。また、図 2 の横軸の全幅で 1 日間のスケールとなっている。同様に、図 3 の横軸は全幅で 1 ヶ月間のスケールとなっている。

図 2 および 3 のピンク色の折れ線グラフがダウンロード速度、青色がアップロード速度であり、いずれも最大値を記録したものである。ダウンロード速度の最大値は、おおよそ 100Mbps～150Mbps を毎日平均して記録しており、期待通りの帯域幅の改善が実現できたといえる。学内で生じていたインターネット接続が遅いという現象も完全に解消した。

2 台の beat で 2 回線を冗長構成しており、片方がリンクダウンした際には、もう片方の回線のみでインターネット接続を維持することが可能になる。また、設定した比率に応じた回線の使用頻度で、2 回線で負荷分散を行っているが、トラフィックの状況に応じた負荷分散はできない。

前述したように、beat には簡易的なメールのウィルスチェックや IPS の機能が備わっており、インターネットから学内 LAN への通信はもちろん、学内 LAN から学外への通信についても、不正な通信を禁止したり記録したりすることができるようになった。インターネットから学内 LAN への攻撃が存在することは予想していたが、学内 LAN からインターネットへの不正通信もそれなりに存在した。多いものは Baidu（百

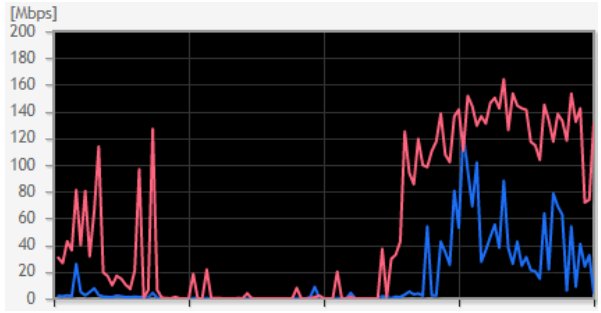

図 2　SINET5 側のルーターによる速度計測（1 日間）

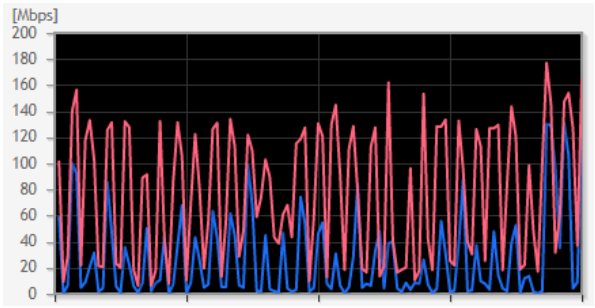

図 3　SINET 側のルーターによる速度計測（1ヶ月間）

度）と Old Adobe Flash Request であり、端末の対策を講じる必要性が認識できた。

3 DNS の運用方法

2 節で述べた SINET5 への接続の際に名前解決をどの様に運用するかについて、検討を重ねる必要が生じた。本節では、その経緯と解決方法を述べたい。

3.1 更新前の名前解決の運用状況

学内 LAN に設置している DNS サーバは、権威サーバの役割として、学内 LAN 上のサーバの名前解決に利用すると共に、フォワーダーとして、旧プロバイダー業者のフルサービスリゾルバを登録していた。また、学内 LAN 上の端末には、DNS サーバの設定として、プライマリに学内 LAN 上の DNS サーバを、セカンダリ以降は、旧プロバイダー業者のフルサービスリゾルバを登録している。この様に設定することで、学内 LAN 上の DNS サーバに障害が発生した場合でも、インターネット接続時の名前解決は維持されるようになっていた。

他方、本学のドメイン管理をしている権威サーバも、旧プロバイダー業者のサービスを契約して利用することで、安定稼働を実現してきた。この契約は今後も継続利用する予定である。

3.2 更新時の問題と解決方法

SINET5 へ接続するに当たり、名前解決に関して次のような問題が生じた。

SINET5 には参照できる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。そのために、SINET5 側の専用線を通じて、インターネット接続する際にも、新プロバイダー業者のバックボーン上にあるフルサービスリゾルバを参照しようとしたが、オープンリゾルバでは無いために SINET 側の専用線に紐づいた IP アドレスで NAT すると参照できなかった。

また、2 回線ともに新プロバイダー業者から借り受けているので、同業者のフルサービスリゾルバを参照できるように設定変更を要求したが、セキュリティ上の問題から、不可能であるとの回答が返ってきた。

学内 LAN 上にフルサービスリゾルバを構築する方法も考えられるが、そのサーバに障害が生じるとインターネット接続ができなくなる事態を避けるためと、障害時のサーバの復旧も迅速に行える体制にないために、従前から、本学と契約関係のあるプロバイダー業者のフルサービスリゾルバを参照することで、名前解決を安定稼働させるという選択をしてきた。

2.2 で述べたように、beat の負荷分散機能は設定比率に応じて、接続する回線の使用頻度を決定している。このとき、一度、片方の回線に振り当てられた端末は、その端末の IP アドレスの第 4 オクテットを記録されて、それを判断基準に、その回線でインターネット接続をし続ける仕様になっている。つまり、学内 LAN 上の DNS サーバが SINET5 側の回線に割り当てられてしまうと、フォワーダーとして設定している新プロバイダー業者のフルサービスリゾルバが参照できないことになってしまう。また、各端末も一度、SINE5 側に割り当てられてしまうと、同様の状態になり、セカンダリとして新プ

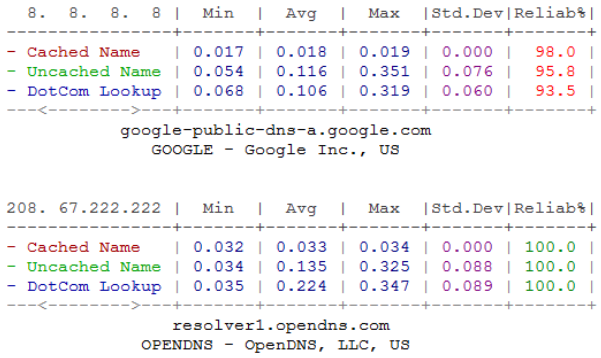

図 4　Google Public DNS と Open DNS の DNS Benchmark のテスト結果

ロバイダー業者のフルサービスリゾルバを設定したとしても、参照することができない。

SINET5 側の回線と商業プロバイダーの回線の帯域幅の比は 100：1 であることから、当然、beat での負荷分散の割合もそれに応じた設定値になる。したがって、インターネット接続は、ほぼ、SINET5 側へ割り当てられてしまうことになるので、この問題は解決しなければならない重要な問題であった。

以上のような理由で、SINET5 側の回線では名前解決に支障が生じていたが、フルサービスリゾルバを参照するときだけは、商業プロバイダー側の 10Mbps 専用線を使用するように beat で静的経路情報を設定することで、この問題を解決した。

4 オープンリゾルバの利用

3.2 で述べたように SINET5 側のインターネット接続における名前解決を、beat に静的経路情報を設定することで解決したが、商業プロバイダー側の回線がリンクダウンしたり、beat1 に障害が発生したりすると、途端に名前解決ができない状態に陥ってしまう。この対策として、緊急時には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 と Open DNS が存在するが、両者を評価した結果、Open DNS を利用することを結論した。本節では、オープンリゾルバを評価することの必要性と、評価方法について説明したい。

4.1 オープンリゾルバに対する注意喚起

3.2 で述べたように、商業プロバイダーが所有するようなフルサービスリゾルバは、その業者から貸与されている IP アドレスからしかアクセスできないように制御されていることが一般的である。このことは、オープンリゾルバがいわゆる踏み台として利用され、サーバ等への DDoS（Distributed Denial of Service）攻撃に利用されていたことへの対策でもあり、本来、オープンリゾルバである必要のない DNS サーバについては、不特定多数の端末からのアクセスを禁止するように推奨されている。以上のことは、JPNIC の「オープンリゾルバ(Open Resolver)に対する注意喚起」というページに詳細な記述がある[1]。

4.2. DNS Benchmark と DNS Spoofability Test

オープンリゾルバである Google Public DNS と Open DNS についての性能と安全性を評価するにあたって、Gibson Research 社の DNS Benchmark と DNS Spoofabilty Test を利用した。

DNS Benchmark はフルサービスリゾルバの名前解決の応答時間について、「Cached Name」「Uncached Name」「DotCom Lookup」の 3 つの測定結果を表示してくれる。「Cached Name」はフルサービスリゾルバにキャッシュされている名前解決の時間を、「Uncached Name」はキャッシュされていない名前解決の時間を、「DotCom Lookup」はフルサービスリゾルバから com サーバへの問い合わせによる名前解決の時間を意味している。

さて、実際に Google Public DNS と Open DNS について DNS Benchmark を行った結果を図 4 に示す。上段の表が Google Public DNS、下段が Open DNS のテスト結果になっている。

いずれの表も、項目が左から、「Min」「Avg」「Max」「Std.Dev」「Reliab%」の順となっており、最初の 3 つは名前解決に要する最短時間、平均時間、最長時間となっており、単位はいず

れも秒である。4 番目の項目は、名前解決に要する時間の標準偏差であり、値が小さいほど、名前解決の時間が均一で安定していることを示している。最後の項目は、クエリに対する応答の信頼性を示している。クエリが消失したり、破棄されたり、無視されたりすると、名前解決に重大な遅延をもたらすことになる。

図 4 の結果が示す通り、名前解決の時間は若干、Google Public DNS の方が短いようであるが、いずれも最長時間は 0.4 秒以内である。また、名前解決の信頼性は、Open DNS は 100%であり、Google Public DNS は数パーセントの欠損がある。

他方、DNS Spoofability Test は主としてキャッシュポイズニングに対する安全性評価を行う Web サービスである[2]。これについては、文献[3]でテスト結果について説明しているので、そちらに譲りたい。

4.3. オープンリゾルバの利用順位

4.2 の DNS Benchmark の結果と文献[3]の DNS Spoofability Test の結果より、Google Public DNS よりも Open DNS を優先して、緊急時に用いることを結論する。その理由は、以下の三点である。

一点目は、DNS Benchmark の結果で示されている、クエリに対する応答の信頼性が、Open DNS の方が勝っている点である。二点目は文献[3]で述べている通りであるが、DNS Spoofability Test で、Google Public DNS よりも Open DNS のポートランダム化の度合いが高いことである。三点目は、実際に Google Public DNS をフルサービスリゾルバとして設定すると、名前解決の遅延が観測されたことである。

5. 名前解決の構成方法の概略

本学の名前解決の構成方法は、前述した通り、学内 LAN 上の DNS サーバにフォワーダーとして、新プロバイダー業者のフルサービスリゾルバを登録していることが根幹である。また、通常の学内端末は、学内 LAN 上の DNS サーバをプライマリに設定している。それに加えて、学内端末の一部は、学内 LAN 上に配備されている L3 Switch の DNS リレー機能を用いて、端末からの名前解決のクエリを学内 LAN 上の DNS サーバをプライマリとして、セカンダリ以降をフルサービスリゾルバへリレーしている。以上の概略を図 5 に示す。

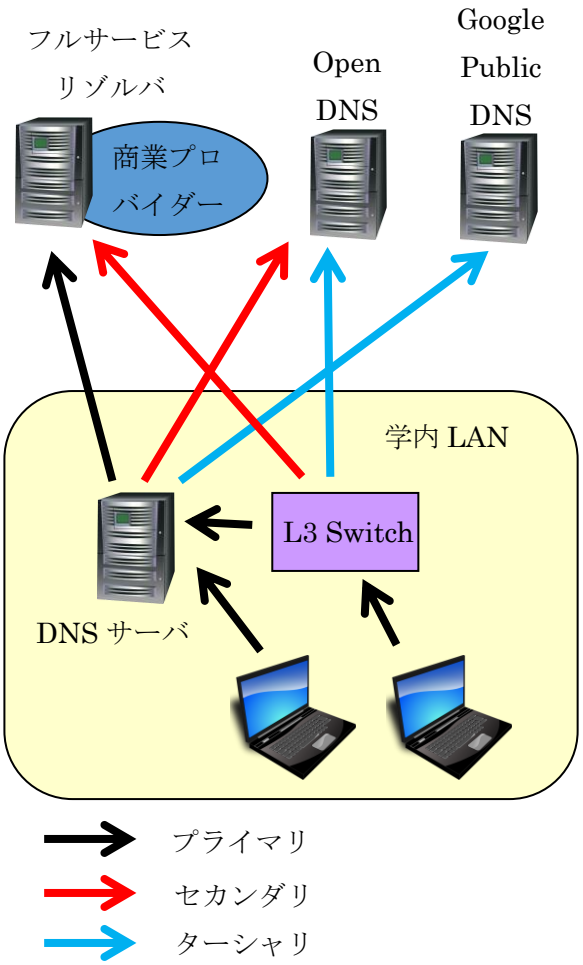

図 5　学内 LAN 上の名前解決の構成方法

学内端末には、旧プロバイダーのフルサービスリゾルバがセカンダリ以降に設定してあったが、今回、回線業者を変更したことにより、本来であれば、セカンダリの IP アドレスを新プロバイダーのフルサービスリゾルバへと変更する必要がある。

学内 LAN 上の DNS サーバが正常稼働している状態では特に問題はないが、障害時には、学

内端末の DNS のセカンダリ以降の設定が新プロバイダーの IP アドレスに変更されていない場合は、途端に名前解決ができない状態に陥ってしまう。その解決策として、L3 Switch の DNS リレー機能を用いて、端末レベルではなく、ネットワークの上位で新プロバイダーのフルサービスリゾルバへリレーすることで、名前解決の冗長構成を実現している。現在は、試験的に学内 LAN 上の約 100 台の端末のみをリレーしている状況である。

6. 更新内容のまとめと今後の予定

本稿では、2016 年度に本学で行ったインターネット接続環境の更新工事について報告した。

2 節では、次のことを述べた。インターネット接続の帯域不足を、SINET5 への接続へと移行することで解消したこと、並びに、その際に用いる回線を新たな業者へと移行したことで、回線費を約 40%削減することができた。それに伴い、更新をしたロードバランサー機能やファイヤーウォール機能についても、高額な専用機ではなく、富士ゼロックス社の beat/active を用いることで、簡易的ではあるが、回線の負荷分散機能や冗長化機能、IPS 機能を配備することができた。また、これらのネットワーク機器に付随する年間固定費も増やさずに済んだ。結果として、「帯域の大幅な増強」「回線費の大幅な削減」「セキュリティの向上」という三点が実現できたメリットの大きい工事となった。

3 節では、SINET5 に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ことより、SINET5 を通じてインターネット接続する場合でも、名前解決だけは商業プロバイダーのフルサービスリゾルバを利用していることを述べた。

4 節では、商業プロバイダーへのインターネット接続に障害が発生した緊急時には、一時的に Open DNS を利用することを採用したことを述べた。

文献[3]では、DNS Spoofability Test のフルサービスリゾルバの安全性評価の方法について、次のように述べている。ある端末で DNS Spoofability Test を実施すると、端末が参照可能なフルサービスリゾルバは、Gibson Research 社がテスト用に準備した権威サーバへ、名前解決の問い合わせを行い、その際に利用したポート番号とトランザクション ID が記録されることになる。このテストを Google Public DNS と Open DNS について複数回テストを繰り返しても、クエリの数が Google Public DNS は Open DNS の 10 分の 1 以下しか記録されない。この現象と、図 4 の DNS Benchmark のテスト結果に示されている「Reliab%」の数値が低いことに関連性があるか否かは不明であるが、本学と契約関係のある商業プロバイダーや著者が自宅で契約している商業プロバイダーのフルサービスリゾルバは、同テストにおいてさらに多い数のクエリを安定して記録している。実際に、両者のクエリの数を比べると、Google Public DNS のクエリの数は、商業プロバイダーの数十分の一程度である。

5 節では、現在の学内 LAN の名前解決方法についてまとめた。学内 LAN 上の DNS サーバに障害が発生した場合の対策として、L3 Switch の DNS リレー機能を利用することで、フルサービスリゾルバの参照を冗長化する構成へと現在、移行中である。L3 Switch のリソースや端末の名前解決時間の状況を観察しながら、問題が生じなければ、全端末をリレーする構成へと、最終的には完全移行することを計画している。

以下、本学のインターネット接続環境について、今後、継続検討や留意が必要な事柄について述べたい。

上記では緊急時に Open DNS を用いて、名前解決することを述べたが、Open DNS は本学と契約関係のないオープンリゾルバである。あるとき、その利用方針が急に変更になり、オープンリゾルバでなくなったり、サービスが廃止になったりすることも十分に考えられる。その様

な事態を想定して、Open DNS を日常的に死活監視することで、障害を示した（参照できない）場合には、その次の対策を、至急、策定する必要がある。DNS Benchmark のサイトからのリンク先[4]には、更に数多くのオープンリゾルバに関する情報がまとめられた CSV ファイルがある。このファイルの情報を DNS Benchmark を読み込むことで、新たに利用可能なオープンリゾルバを探索するのに、大いに役立つものと思われる。

現在、名前解決以外のインターネット接続に関しては、ほぼ、SINET5 側の回線を利用する設定を行っている。この回線は、本学と SINET5 の福岡 DC2 を結ぶ専用線であり、その両端に設置しているメディアコンバーターは、RJ45 と 1000BASE-LX を変換する仕様である。帯域幅は実質的にはメディアコンバーターの性能によって制限されているので、将来的にこの回線に帯域不足が生じた場合には、回線工事の必要はなく、メディアコンバーターやルーターなどのスループットを改善すればよいことになる。

参考文献

[1] https://www.nic.ad.jp/ja/dns/openresolver/
[2] https://www.grc.com/dns/dns.htm
[3] 田中健吾、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、大学 ICT 推進協議会 2017 年度年次大会、2017 年.
[4] http://www.GRC.com/dns/resolvers.csv