DNS のデータ整理と DoH の試験的運用

一瀬 光 [1)], 中島 順美 [1)], 瀬戸 桂 [1)], 吉永 千有希 [1)], 吉崎 弘一 [1)]

1) 大分大学 学術情報拠点　情報基盤センター

center@oita-u.ac.jp

Organizing data and supporting DoH on DNS

Hikaru Ichise[1)], Junmi Nakashima[1)], Katsura Seto[1)], Chiaki Yoshinaga[1)], Koichi Yoshizaki[1)]

1) Information Technology Center, Oita Univ.

概要

各大学ではドメイン名と IP アドレスを変換するために DNS を利用・管理している。ネットワーク管理者がサブドメイン等と IP アドレスを DNS に登録し、日々運用している一方で、利用されなくなったサブドメインや IP アドレスまで登録し続けている状況が発生している。そこで、本大学の運用で今年度その利用されなくなったサブドメインと IP アドレスに着目し、各学部、事務組織に現状の確認し、DNS から一括削除を行った知見を報告する。更に、DNS の問合せに関するプライバシーの懸念事項を考慮し、全大学初だと思われる DoH（DNS over HTTPS）の試験的運用を行ったことを報告する。

1　はじめに

現代のインターネットの利用において、DNS(Domain Name System) は最も不可欠なツールの一つになっている。DNS の重要な役割として、ドメイン名から IP アドレスに変換する（名前解決と呼ぶ。）ために利用されている [1]。それによって、インターネットユーザは Web 閲覧、メール送信、多様なアプリケーション等を容易に利用することができる。

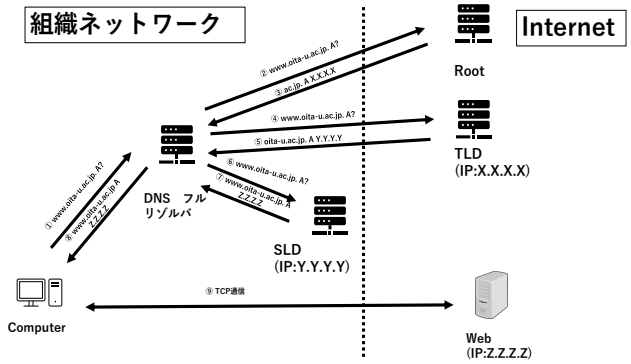

図 1　DNS の挙動概要と Web 閲覧方法

図 1 はコンピュータが名前解決して、メールや Web 閲覧を利用する方法を示す。初め、組織内のコンピュータは「www.oita-u.ac.jp」のドメイン名の IP アドレスを取得するために、DNS フルリゾルバに対し、DNS クエリを送信する（矢印　①）。尚、「www.oita-u.ac.jp」のドメイン名の IP アドレスを取得する際には A レコードと呼ばれる正引きを利用する。次に、DNS フルリゾルバは各権威 DNS サーバ（Root、TLD（Top Level Domain）、SLD（Second Level Domain））に対して、Root の権威サーバから順次 SLD まで DNS クエリと DNS レスポンスを送受信し、名前解決を行う（矢印 ② 〜　矢印 ⑦）。これを反復問い合わせと呼ぶ。最終的に SLD の権威 DNS サーバは「www.oita-u.ac.jp」のドメイン名と対応する IP アドレス「Z.Z.Z.Z」を DNS フルリゾルバに返す（矢印 ⑧）。これを再帰的問い合わせと呼ぶ。コンピュータは DNS フルリゾルバからその IP アドレス「Z.Z.Z.Z」を受け取り、その後、「Z.Z.Z.Z」のサーバに接続し、Web の閲覧を行うことができる（矢印 ⑨）。このようにして、メールも同様の手続きで名前解決により、メールサーバを特定して、コンピュータはメール送受信を行うことができる。尚、メールサーバを特定する際には A レコードだけでなく、MX レコードと呼ばれるレコードも利用する。

組織内のネットワーク管理者は自身のドメイン配下の権威 DNS サーバと DNS フルリゾルバを常に運用・管理することによって、永続的にインターネットを利用できるような環境を教職員、学生に提供している。大学組織によっては SLD だけでなく、Third Level Domain 以下のサブドメインを持つ組織体系（各学部、研究科、事務部局等）を構成し、サブドメインの持つ権

威 DNS サーバをその組織が運用しているところもある [2]。権威 DNS サーバには自組織に存在する Web サーバ、メールサーバ、アプリケーションサーバ等のドメイン名と IP アドレスを登録することによって、教職員、学生だけでなく、一般のインターネットユーザからも利便性のあるシステムになっている。しかしながら、一方で以下のことがネットワーク管理者の課題として挙げられる。

- システム管理者が構築した Web サーバ、アプリケーションサーバ等が時を経て、利用されなくなったり、リプレイスにより、ドメイン名と IP アドレスが利用されなくなること
- システム管理者が人事異動等で既に不在になっていること
- システム管理者による申請当時の申請書のサブドメインを把握していないこと

そういった場合、DNS を管理している情報基盤センターのネットワーク管理者には連絡がされずに、権威 DNS サーバにドメイン名と IP アドレスが残されたままになり、そこをついて、不正通信や外部からの攻撃が発生する可能性もある [4]。JP ドメインを管理する JPRS では、DNS サーバとして使用していたホスト名が、ドメイン名の廃止によって存在しなくなったあとも DNS サーバとしてレジストリに登録したままであるなどの管理ミスにより、DNS サーバが属するドメイン名の管理権限を第三者が取得し、本来のサイトと異なるサイトに誘導できるという危険性が指摘しており、その原因は「DNS サーバ管理が不十分であることにより引き起こされる問題」ことを報告している [3]。

そこで、そういったことを考慮し、本稿の目的はセキュリティの面からも権威 DNS サーバのデータの整理をすることによって、学内のネットワーク環境の安全性を高めることである。これまで、本大学（大分大学）ではドメイン名と IP アドレスを権威 DNS サーバに登録後に、削除依頼されることはなく、現在もそのドメイン名と IP アドレスが利用されているのか不透明であった。そのため、本学の権威 DNS のゾーンには約 5000 件のデータが登録されていた。本稿ではそのゾーンのデータを見直し、利用されていないデータは削除するシステム、手続きを行った。その結果、約 500 件のデータまで減らすことができたことを報告する。更に、併せて昨今の DNS 通信の暗号化の方向に向いている、そこで、本学でも他大学では行っていないであろう DoH（DNS over HTTPS）[5] の運用を試験的に開始し、その状況も報告する。

2　データ整理の手続き

前章ではセキュリティの面から権威 DNS サーバはドメイン名に対する DNS サーバ管理が不十分により大きな問題が発生することを述べた。そこで、その権威 DNS サーバの管理を再度見直すことを目的として、本章では本学で行った、権威 DNS サーバのデータ整理について説明する。

本学では DNS として BIND を利用しており、ドメイン管理の全体は以下のように管理している。

- oita-u.ac.jp: 大分大学情報基盤センターが管理している全体のドメイン名（権威サーバ）
- csis.oita-u.ac.jp, dxhr.oita-u.ac.jp: 大分大学理工学部知能情報システムプログラム, DX 人材育成プログラムが管理しているサブドメイン名（権威サーバ）
- med.oita-u.ac.jp: 大分大学医学情報センターが管理しているサブドメイン名（主に医学部管理）

そこで、今回の権威 DNS サーバのデータ整理を行った対象として、情報基盤センターが管理している「oita-u.ac.jp」とし、その中のデータを整理することとした。尚、「csis.oita-u.ac.jp」、「dxhr.oita-u.ac.jp」については我々の手の届かない範囲であり、かつ、別のサーバであるため、整理することは難しく、理工学部知能情報システムプログラムという範囲が限られているため、管理者は容易に整理することが可能であると考えれる。実際に、その管理者もその後、整理しているという証跡も取っている。更に、「med.oita-u.ac.jp」については別の部署であるが、常に情報基盤センターと連携を取っているため、管理できている。更に、毎年 Web サーバ等のサーバ証明書を義務付けしているため、取得しているサーバについては権威 DNS のドメイン名を削除対象外とした。

情報基盤センターが管理している「oita-u.ac.jp」における権威 DNS サーバとして、今回行った手続きは以下のように行う。

(1)　学内のポータルにて「ホスト名の調査依頼」としてドメイン名と IP アドレスの見直す全体周知
(2)　システム管理者および関係者は学内の申請フォームから申請依頼
(3)　情報基盤センターで削除スクリプトを作成し、権威 DNS サーバからスクリプトにて削除

（1）については図 2 に示す大分大学にて運用されている WEBWALKER という学内ポータルの掲示板にて全体周知で案内する。こちらは初め学内メールで案内することを検討したが、昨今不審メールや標的型メールに関する報告も多いため、それを避けるために、学内ポータルにて全体周知を行うこととなった。（2）は（1）の全体周知から学内ユーザが認証付きの申請 Web フォーム図 3 から残しておきたいドメイン名と IP アドレスを新規申請する。上記の（1）と（2）については全体周知から申請終了の期間を約 1 ヶ月間とする。つまり、5 月の中旬に全体周知を行い、6 月中旬までには申請フォームから申請することとし、それまでに申請していないドメイン名は全て権威 DNS から削除する旨、通達する。その申請終了期間までの 1 ヶ月で削除プログラムを作成し、削除プログラムは申請フォームからのドメイン名と IP アドレスのリストを取得し、その後、そのリスト以外のものはゾーンから削除するというシェルスクリプトである。（3）では実際に 6 月中旬以降に作成したシェルスクリプトを起動し、削除する。本手順を行うことにより、現状に見合ったドメイン管理ができると考えた。

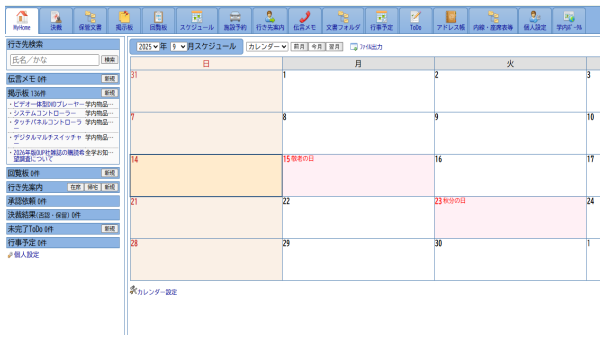

図 2　学内ポータル

図 3　申請フォーム

表 1　データ削除結果

	データ数
データ削除前	約 5000
データ削除後	約 500

3　データ整理の運用と結果とその課題

本章では前章で述べたデータ整理に関する手続きを実際に行ったことを基に、その結果とその課題を報告し、今後も実運用するための考察を行う。

データ整理を実際に 4 月から検討し、約 3 ヶ月をかけて行った。実際に 5 月中旬に全体周知を行った結果、これまで認識していないユーザ、特に事務職員からの問い合わせが数件の問い合わせがあったが、業務的に情報基盤センターに負荷がかかるということはなかった。実際に権威 DNS サーバからユーザから依頼された通り、つまり、申請されたいないデータを削除した結果は表 1 に示す。データ数を確認すると、削除前に約 5000 件あったレコードは削除後に確認すると約 500 件に大幅に削減できたことを示す。この結果、不必要な権威 DNS のデータは想定通り大幅に削除されており、外部からアクセスできるシステムも減らされて、より一層大分大学のネットワークの安全性が高まった可能性がある。

しかしながら、削除したことにより、一部の教員から、自身のシステムに接続できないという問い合わせも来ており、その教員は学内ポータルも参照していないことが発覚した。その教員については再度、申請フォームから自身のシステムのドメイン名と IP アドレスを申請していただくことを推奨した。その他の課題としては、学内のクライアントコンピュータにまで権威 DNS サーバに登録しているものもあったため、今後は登録しないように依頼するように検討している。この運用を毎年 4 月から 6 月にかけて、運用していくことで不必要なドメイン名を適宜削除でき、適切な管理ができると考えられる。

4　DoH の運用

前章で権威 DNS サーバのデータ整理に着目してきたが、同じ DNS でも本章では DNS フルリゾルバに着目して、昨今 DNS の通信が暗号化がされてきたので、本学でも暗号化の運用を行ったことを報告する。

昨今、IETF（Internet Engineering Task Force）では「広範囲にわたる監視は攻撃である」と定義 [6] されて、多くの通信が暗号化されるようになってきた。IETF ではプロトコルの設計により、その攻撃を軽減

することが明記され、求められている。最も一般的に暗号化されたのは HTTP である。2000 年以降 HTTP は HTTP over TLS が RFC2818 で定義されて [7]、昨今では HTTP over SSL/TLS がほとんどの Web サーバで採用されている。しかしながら、DNS サーバとの通信では依然として平文で行われている。漸く 2018 年以降に RFC にて DNS 通信の暗号化が標準化された [5]。通信を暗号化することによって、中間者攻撃からの防御や通信内容が外部から容易に傍受されるリスクが低減できる利点があり、今後も多くのプロトコルが暗号化されていく方向になる。一方で、DoH は現在、コンピュータから DNS フルリゾルバまでの間を暗号化することができる。コンピュータの設定も必要だが、DNS フルリゾルバの証明書の埋め込みや config の設定も必要であるため、専門的なネットワーク管理者でしか運用・管理できないような環境になっており、既存では大学において実装していることは報告されていない。尚、Google [8]、Cloudflare [9]、Quad9 [10] のパブリック DNS では既に DoH が実装されており、利用することも可能である。

そこで、本大学では他大学に先駆けて、プライバシーの保護の観点から DoH の設定をサーバ側に実装し、ユーザに利用してもらうことを目的として、DNS フルリゾルバ側の設定を行った。行った手順としては以下である。

(1) DNS フルリゾルバ側の設定ファイルと電子証明書の設定
(2) 学内ユーザに向けてのコンピュータの設定方法

（1）では DNS フルリゾルバの BIND の設定ファイルに「tls local-tls」に証明書の指定と「https-port 443;」のオプションを設定することで可能にできる [11]。更に、電子証明書は OpenSSL により RSA2048 の CSR を作成し、その後、NII のサーバ証明書の発行申請を行った後に、その鍵を DNS フルリゾルバにインストールするというものである。（2）では Windows11 に特化して、DoH を利用したいユーザの設定方法のマニュアルを情報基盤センターのサイトで図 4 のように公開した。尚、本設定はオプションであるため、情報基盤センターでは DoH の具体的なサポートは行わないこととした。

このような設定を行ったが、現状ユーザからの問い合わせに関してはなかった。今後は DNS フルリゾルバの負荷の状況や学内ユーザがどれくらい利用しているかの統計も取っていく方向である。更に、暗号化方法として DNS over QUIC（DoQ）も検討されているようなので、DoQ に向けて、実装と学内デプロイしていくかも検討する。

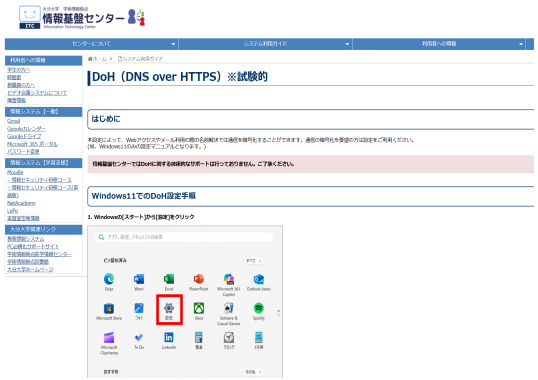

図 4　DoH 設定マニュアル

5　終わりに

本稿では大分大学における DNS の昨今のデータ整理に関する報告と DNS フルリゾルバにおける DoH の試験的実装を行った旨を報告した。DNS のデータ整理は多くのデータが登録されてあったため、不必要なデータは学内ユーザに確認しながら、削除し、全体を見直す形で健全化することができた。一部のユーザからの問い合わせもあり、今後の課題が明確化することができた。DNS のデータ整理により、セキュリティの安全性を保つことができる一因にもなった。また、個人のプライバシーの保護の観点から DoH のサーバ側の設定を行い、ユーザに対して DoH の設定方法についても HP で提供した。

今後は DNS のデータ整理を NetBox 等で管理し、自動化と手続きの簡略化の検討を行う。更に DoH についてはユーザ数の確認と DNS フルリゾルバ側の負荷についても確認する。

参考文献

[1] P. Mockapetris, DOMAIN NAMES - CONCEPTS AND FACILITIES, IETF RFC1034, Nov 1987.
[2] 山守一徳, 平田和之, セキュリティ対策のための大学内一括管理向け DNS 登録システムの開発, 学術情報処理研究, 2003, 7 巻, 1 号, p. 13-22.
[3] JPRS, DNS サーバの不適切な管理による危険性解消のための取り組みについて, https://jprs.jp/whatsnew/notice/before2011/problematic_ns.html （2025 年

9 月 12 日）.
[4] 関谷勇司, 石原知洋, DNS のセキュリティ対策と運用状況の調査ツール, 情報処理学会誌,Vol.41,No.12,pp.1373-1379 （Dec 2000）.
[5] P. Hoffman, P. McManus, DNS Queries over HTTPS （DoH）, IETF RFC8484, Oct 2018.
[6] S. Farrell, H. Tschofenig, Pervasive Monitoring Is an Attack, IETF RFC7258, May 2014.
[7] E. Rescorla, HTTP Over TLS, IETF RFC2818, May 2000.
[8] Google, Introduction to Google Public DNS., https://developers.google.com/speed/public-dns/docs/intro（2025 年 9 月 12 日）.
[9] Cloudflare, Introduction to Cloudflare Public DNS, https://www.cloudflare.com/learning/dns/what-is-1.1.1.1/ （2025 年 9 月 12 日）.
[10] Quad9, An open DNS recursive service for free security and high privacy, https://quad9.net （2025 年 9 月 12 日）.
[11] ISC, BIND Implements DoH, https://www.isc.org/blogs/bind-implements-doh-2021/ （2025 年 9 月 12 日）.