# DNSいったい
# DoH（どう）するの！？

## ～とあるプロトコル改変に関わる考察～

Tomofumi Okubo

Distinguished Engineer, Industry Relations

DigiCert, Inc.

# DNS-Over-HTTPS

- RFC8484 DNS Queries over HTTPS (DoH)
- DNSの問い合わせをHTTPS経由で行う
- 各々のアプリケーションが好みの再帰リゾルバを設定できる
- アプリケーションと再帰リゾルバ間で応答が暗号化される
- ウェブ関係者の発案（DNS関係者でない）

# はやくもFireFoxがDoH対応

mozilla wiki

Page Discussion Read View source View history Search

Main page
Product releases
New pages
Recent changes
Recent uploads
Random page
Help

How to Contribute
All-hands meeting
Other meetings
Contribute to Mozilla
Mozilla Reps
Student Ambassadors

MozillaWiki
About
Team
Policies
@MozillaWiki
Report a wiki bug

Around Mozilla
Mozilla Support
Mozilla Developer Network
Planet Mozilla
Mozilla Blog
Research

Tools
What links here
Related changes

## Security/DOH-resolver-policy

< Security

Contents [hide]

1 Mozilla Policy Requirements for DNS over HTTPs Partners
1.1 Privacy Requirements
1.2 Transparency Requirements
1.3 Blocking & Modification Prohibitions
2 Enforcement

### Mozilla Policy Requirements for DNS over HTTPs Partners

This document describes the minimum set of policy requirements that a party must satisfy to be considered as a potential partner for Mozilla's Trusted Recursive Resolver (TRR) program. It specifically describes data collection and retention, transparency, and blocking policies and is in addition to any contractual, technical or operational requirements necessary to operate the resolver service.

#### Privacy Requirements

Mozilla's TRR is intended to provide better, minimum privacy guarantees to Firefox users than current, ad hoc provisioning of DNS services. As such, resolvers must strictly limit data collection and sharing from the resolver. More specifically:

1. The resolver may retain user data (including identifiable data, data associated with user IP addresses, and any non-aggregate anonymized data) but should do so only for the purpose of operating the service and must not retain that data for longer than 24 hours.
   - Only aggregate data that does not identify individual users or requests may be retained beyond 24 hours.
2. The resolver must not retain, sell, or transfer to any third party (except as may be required by law) any personal information, IP addresses or other user identifiers, or user query patterns from the DNS queries sent from the Firefox browser.
3. The resolver must not combine the data that it collects from queries with any other data in any way that can be used to identify individual end users.

https://wiki.mozilla.org/Security/DOH-resolver-policy

# DoHが解決をしようとしていること

- プライバシーとセキュリティのため（盗聴・検閲対策）
- DNSのパフォーマンスに対する不満

# 問題点

- DNSのフィルタリングが利かなくなる
- インターネットのフラグメンテーション
- アプリケーションが選択するリゾルバの品質が悪いかも
- インシデントや障害が起こった時のトレースが困難になる
- 内部DNSがうまく使えなくなる
- C&Cに使えて、マルウェア制作者は大喜び？
- TLSの電子証明書ってDNS使ってるんですけど
- DNSSECがまだきちんと普及していない

# 疑問：RFC8484

[Docs] [txt|pdf] [draft-ietf-doh-...] [Tracker] [Diff1] [Diff2] [Errata]

PROPOSED STANDARD
Errata Exist

Internet Engineering Task Force (IETF)
Request for Comments: 8484
Category: Standards Track
ISSN: 2070-1721

P. Hoffman
ICANN
P. McManus
Mozilla
October 2018

**DNS Queries over HTTPS (DoH)**

Abstract

This document defines a protocol for sending DNS queries and getting DNS responses over HTTPS. Each DNS query-response pair is mapped into an HTTP exchange.

https://tools.ietf.org/html/rfc8484

# 疑問：DNSのプライバシーの評価

[Docs] [txt|pdf|xml|html] [Tracker] [Email] [Diff1] [Diff2] [Nits]

Versions: 00 01 02 draft-ietf-dprive-eval

Network Working Group
Internet-Draft
Intended status: Informational
Expires: April 20, 2016

A. Mohaisen
SUNY Buffalo
A. Mankin
Verisign Labs
October 18, 2015

**Evaluation of Privacy for DNS Private Exchange**
**draft-am-dprive-eval-02**

Abstract

The set of DNS requests that an individual makes can provide a monitor with a large amount of information about that individual. DNS Private Exchange (DPRIVE) aims to deprive this actor of this information. This document describes methods for measuring the performance of DNS privacy mechanisms, particularly it provides methods for measuring effectiveness in the face of pervasive monitoring as defined in RFC7258. The document includes example evaluations for common use cases.

https://tools.ietf.org/html/draft-am-dprive-eval-02

# 疑問

- 本当にエンタープライズでの使用に耐えるものなのか？
- 本当にそれほどプライバシーの保護に役に立つのか？
- 本当にセキュリティの改善につながるのか？
- 解決しようとしている問題より、さらに深刻な問題を作り出してはいないか？
- いきなりプロダクションでデプロイする前にもう少し考えたほうがよくはないか？

# 似たような現象

- TLS1.３の企業での使用についての問題

# お願い

- まずはメーリングリストに参加して議論をモニタリング
- とにかく声を上げることが重要
- 現地に行かなくてもリモート参加が可能
- ただし深い議論をするには現地に行くことが必須

声の大きい人が得をして、黙ってると恐ろしいことがどんどん決まって行ってしまう。そんな一面もあるIETF。

ご静聴ありがとうございます。

tomofumi.okubo@digicert.com