

DNSの「明日のカタチ」について考える

～ランチのおともにDNS～

2022年6月24日

Internet Week ショーケース 徳島・オンライン
株式会社日本レジストリサービス (JPRS)

森下 泰宏

本セミナーはInternet Week 2021 ランチタイムウェビナーのUpdate版です

ショーケースでも「ランチのおともにDNS」！

- Internet Week ショーケースの歴史（今回で6回目）
 - 第1回：2017年6月1日・2日 @ 名古屋
 - 第2回：2018年5月31日・6月1日 @ 広島
 - 第3回：2019年5月30日・31日 @ 仙台
 - 第4回：2020年7月9日・10日 @ オンライン
 - 第5回：2021年7月8日・9日 @ オンライン
 - **第6回：2022年6月23日・24日 @ 徳島・オンライン**

3年ぶりの現地開催、おめでとうございます！
都合によりオンラインでの参加となり、残念です

今年はヒューリックホールの壇上に立ちたいです！

講師自己紹介

- 森下 泰宏（もりした やすひろ）
 - 所属：JPRS 技術広報担当・技術研修センター
 - 主な業務内容：技術広報活動全般・社内外の人材育成



<略歴>

1988年	デジタルコンピュータ株式会社（DCL、独立系SIer）に入社 1990年よりWIDE Projectメンバーとして、日本のインターネット構築に創始期より参加。
1993年	学校法人東京理科大学情報処理センター着任 キャンパスネットワーク及び教育用システムの設計、構築、運用を行う。
1998年	社団法人日本ネットワークインフォメーションセンター（JPNIC）着任 JPドメイン名登録システム及びJP DNSの管理運用に従事。
2001年	株式会社日本レジストリサービス（JPRS）に転籍 DNSに関する技術研究を中心に活動。
2007年	同社技術広報担当として、DNSおよびドメイン名関連技術に関する情報提供・教育啓発を中心に活動中（現職）。
2021年	同社技術研修センター主任講師として、教育・研修を通じた社内外の人材育成を担当（兼務・現職）。

本日の内容

1. 誕生当時のDNSとその進化のカタチ
2. 今日のDNSのカタチ
3. 明日のDNSのカタチとは

注：本資料で紹介するRFCはそれぞれの初版であり、新版がリリースされている場合があります

1. 誕生当時のDNSとその進化のカタチ

このパートの内容

- 誕生当時のDNSとその進化のカタチについて、
プロトコル・実装・運用の観点から振り返る
 - 誕生当時のDNSのカタチ
 - DNSの進化のカタチ
 - まとめ：誕生当時のDNSとその進化のカタチ



DNSが誕生した1983年に発売
(画像引用元：Wikipedia)

誕生当時のDNSのカタチ（プロトコル）

- **設計思想**

- 動かすことが優先、悪意の存在を想定せず

- **データ形式**

- 1セッションでやりとりされる問い合わせ・応答は1セット
- 通信のやりとりは平文

- **問い合わせ方法**

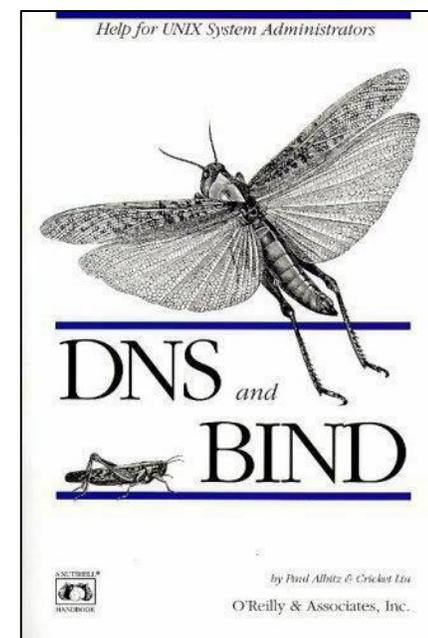
- 最初はUDPで、切り詰めを検出した後にTCPで再問い合わせ
- 名前解決の際、クライアントから受け取った内容をそのまま問い合わせ

- **UDPメッセージサイズ最大値**

- 問い合わせ・応答が1パケットに収まるよう、512バイトに制限

誕生当時のDNSのカタチ（実装）

- 最初に広まった実装：**BIND**（1985年）
 - 当初、オープンソースのDNSソフトウェアはほぼBINDのみ
 - BINDの動作・運用上の制限が、DNSの仕様・運用にも影響
 - リゾルバーライブラリ（libresolv）が付属
 - 最初期は各自が明示的にリンク
 - 後に標準Cライブラリ（libc）に組み込み



誕生当時のDNSのカタチ（運用）

- **目標**：HOSTS.TXTによる集中管理の置き換え
- **権威DNSサーバー間の同期**：30分～1時間ごと
 - ゾーンの管理者がSOAレコードで設定
- **更新間隔**：TLDレジストリでは1日に1～2回程度
- **普及のポイント**：メール配送への利用
 - sendmailがMXレコードによるメール配送を標準サポートしたことで、DNSの普及が進んだ

DNSの進化のカタチ

- インターネットの急速な普及に対応する形で進化
 - **プロトコル**：足りない機能の追加、新たなニーズへの対応
 - **実装**：実装の多様化
 - **運用**：信頼性・利便性の向上

DNSの進化のカタチ（プロトコル） 足りない機能の追加（1/2）

- **AAAAレコード・ip6.int**（RFC 1886：1995年）
 - IPv6サポート（正引き・逆引き）追加
- **ip6.arpa**（RFC 3152：2001年）
 - IPv6サポート（逆引き）ゾーンの変更
- **差分ゾーン転送**（RFC 1995：1996年）
 - ゾーン転送の効率化

DNSの進化のカタチ（プロトコル）

足りない機能の追加（2/2）

- **DNS NOTIFY**（RFC 1996：1996年）
 - 権威DNSサーバー間の同期時間の短縮
- **ネガティブキャッシュ**（RFC 2308：1998年）
 - 不在応答をキャッシュし、名前解決の効率を向上
 - RFCの発行前から開発・実装

DNSの進化のカタチ（プロトコル）

新たなニーズへの対応

- **Dynamic Update**（RFC 2136：1997年）
 - クライアントからの動的更新に対応
- **SRVレコード**（RFC 2782：2000年）
 - サービスの登録・サービスの検索に対応
- **国際化ドメイン名**（RFC 3490～3492：2003年）
 - 非英語圏の利用者のニーズに対応
- **DNS64**（RFC 6147：2011年）
 - IPv6の普及促進に対応

DNSの進化のカタチ（実装）

実装の多様化

- **djbdns**（1999年）

- 後の実装で主流になった設計をいち早く採用

- 権威DNSサーバーとフルリゾルバーのプロセス分離

- シンプルで小さい権威DNSサーバー

- フルリゾルバーにおけるソースポートランダムイゼーション、など

- その後、さまざまなDNSソフトウェアが公開

- **PowerDNS**（1999年、2002年にオープンソース化）

- **NSD**（2002年） ・ **Unbound**（2008年）

- **Knot DNS**（2011年） ・ **Knot Resolver**（2016年）

DNSの進化のカタチ（運用）

信頼性・利便性の向上（1/2）

- **IP Anycastの適用**
 - 負荷分散、冗長化、応答時間の短縮
 - 攻撃の局所化・効果抑制
- **IPv6トランスポートへの対応**
 - IPv6でDNSサービスを提供

DNSの進化のカタチ（運用）

信頼性・利便性の向上（2/2）

- **AAAAレコードの登録・取り次ぎ**
 - レジストリ・レジストラにおけるIPv6サポート
- **レジストリにおける更新間隔の短縮**
 - ドメイン名の利便性向上
 - .com/.net：2004年
 - .jp：2006年

JP DNSの更新間隔短縮の実施について
<<https://jprs.jp/whatsnew/notice/before2011/200604-dns.html>>

まとめ：誕生当時のDNSとその進化のカタチ

- **軽量、かつシンプルなプロトコル**として誕生
- **インターネットの普及と共に進化**
- **プロトコル・実装・運用**の進化を経て、今日のDNSに
 - プロトコル：**機能の追加・新たなニーズへの対応**
 - 実装：**BINDの時代から、多様な実装の時代**に
 - 運用：**信頼性・利便性の向上**

2. 今日のDNSのカタチ

このパートの内容

- DNSが今日を迎えるまでに起こった変化の内容と、それらの理由について解説する
 - 今日のDNSのカタチ
 - DNSに起こった変化
 - 変化の理由
 - まとめ：今日のDNSのカタチ

再掲：誕生当時のDNSのカタチ（プロトコル）

- **設計思想**

- 動かすことが優先、悪意の存在を想定せず

- **データ形式**

- 1セッションでやりとりされる問い合わせ・応答は1セット
- 通信のやりとりは平文

- **問い合わせ方法**

- 最初はUDPで、切り詰めを検出した後にTCPで再問い合わせ
- 名前解決の際、クライアントから受け取った内容をそのまま問い合わせ

- **UDPメッセージサイズ最大値**

- 問い合わせ・応答が1パケットに収まるよう、512バイトに制限

今日のDNSのカタチ（プロトコル）

- **設計思想**

- 悪意の存在を想定、対策を追加

- **データ形式**

- TCP接続において、複数の問い合わせ・応答のやりとりが可能に
- スタブリゾルバー⇔フルリゾルバー間の通信を暗号化

- **問い合わせ方法**

- 最初からTCPで問い合わせ可能に
- 名前解決の際、クライアントから受け取った内容を最小化

- **UDPメッセージサイズ最大値**

- 512バイトよりも大きなサイズに拡大可能に

DNSに起こった変化（基本プロトコルの変更）

- **DNS Transport over TCP**（RFC 7766：2016年）
 - 最初からTCPで問い合わせ可能に
 - DNS over TLS・DNS over HTTPSの前提
- **edns-tcp-keepalive**（RFC 7828：2016年）
 - 1セッションで複数の問い合わせ・応答をやりとり可能に
- **EDNS0**（RFC 2671：2000年）
 - UDPメッセージサイズ最大値の拡大
 - DNSに機能拡張のための仕組みを提供

DNSに起こった変化 (DNS以外のサービスとの連携)

- **SPF** (RFC 4408 : 2006年)
DKIM (RFC 4871 : 2007年)
DMARC (RFC 7489 : 2015年)
 - 電子メールサービスとの連携
- **CAAレコード** (RFC 6844 : 2013年)
 - 証明書発行サービスとの連携
- **EDNS Client Subnet** (RFC 7871 : 2016年)
 - CDNサービスとの連携

DNSに起こった変化 (セキュリティ機能の追加 (1/2))

- **DNSSEC** (RFC 4033~4035 : 2005年)
 - 公開鍵暗号技術を用いた署名を付加し、DNS応答の偽装を防止
 - ルートゾーンは2010年、.jpは2011年にDNSSECを導入
- JPRSがJPドメイン名サービスにDNSSECを導入
<<https://jprs.co.jp/press/2011/110117.html>>
- **DNSクッキー** (RFC 7873 : 2016年)
 - DNSメッセージに小さなデータを付加し、通信相手を相互に認証

DNSに起こった変化 (セキュリティ機能の追加 (2/2))

● 応答レートの制限 (DNS RRL) (2012年～)

- 設定した条件により、権威DNSサーバー・フルリゾルバーからの応答レートを制限
- DNSリフレクター攻撃の効果抑制

● 問い合わせレートの制限 (2014年～)

- 設定した条件により、フルリゾルバーから権威DNSサーバーへの問い合わせレートを制限
- ランダムサブドメイン攻撃の効果抑制

DNSに起こった変化（プライバシー機能の追加）

- **DNS over TLS**（RFC 7858：2016年）
DNS over HTTPS（RFC 8484：2018年）
DNS over QUIC（RFC 9250：2022年）
 - スタブリゾルバー⇔フルリゾルバー間のDNS通信の暗号化
- **QNAME minimisation**（RFC 7816：2016年）
 - 権威DNSサーバーへの問い合わせ内容の最小化（秘匿）

DNSに起こった変化（利用者のアクセス抑制）

- **DNS Response Policy Zones (DNS RPZ)**（2010年）
 - ポリシーにより、クライアントに返すDNS応答の内容を制御
 - DNSファイアウォールに利用可能
- **DNSファイアウォール**（2010年代～）
 - DNSを用いたアクセス制御（フィルタリング・ブロッキング）
 - 問い合わせの内容をチェックし、利用者のアクセスを抑制

DNSに起こった変化（外部DNSサービスの登場）

- **パブリックDNSサービス**

- （Google Public DNS : 2009年）

- インターネット利用者に、**名前解決サービス**を提供

- **マネージドDNSサービス**

- （Cloudflare : 2009年、Amazon Route 53 : 2010年）

- ドメイン名登録者・管理者に、**ゾーン管理サービス**を提供

ここまでに出来て来た変化の項目

- 基本プロトコルの変更
- DNS以外のサービスとの連携
- セキュリティ機能の追加
- プライバシー機能の追加
- 利用者のアクセス抑制
- 外部DNSサービスの登場

それらの変化の理由は？

変化の理由（基本プロトコルの変更）

- **インターネットの変化に対応したい**
 - インターネット自身の変化に伴い、DNSに対する要求事項も変化
- **変化に対応するさまざまな仕組みを作りやすくするため、
プロトコル上の制限を緩和**

変化の理由（DNS以外のサービスとの連携）

- **DNSが提供する機能を、DNS以外のサービスでも利用したい**
- サービスの例
 - 電子メールサービス
 - サーバー証明書サービス
 - CDNサービス

変化の理由（セキュリティ・プライバシー）

- **セキュリティ・プライバシーに関する機能を追加したい**
 - 誕生当時、悪意の存在を想定していなかった
 - RFC 1034・1035には「security」「privacy」という単語はない
- 誕生当時のDNSにはなかった機能を、**後付けで追加**
- 後付けで追加したことで、以下の特徴を持つものが多い
 - 複雑なプロトコル仕様
 - 大がかりな実装
 - 体力を要する運用

変化の理由（利用者のアクセス抑制）

- **望まない相手には、接続させないようにしたい**
 - 本来は接続するために使うDNSを、**接続させないために使う**
- **接続させないようにするための機能を、後付けで追加**

変化の理由（外部DNSサービスの登場）

- **サービス利用者とサービス提供者のニーズの一致**
 - 高機能・高性能・安定・安全なサービスの利用・提供
 - なぜ、パブリックDNSサービスは無償で提供されるのか？
- **DNS運用コストの増加**
 - DNSの多機能化
 - DNS運用に要求されるサービスレベルの高まり

まとめ：今日のDNSのカタチ

- **インターネットの変化を受け、DNSのカタチも変化**
 - **みんなの期待に応える**（他のサービスとの連携）
 - **付け入られる隙をなくす**（セキュリティ・プライバシーへの対応）
 - **望まない相手には接続させない**（フィルタリング・ブロッキング）
 - **色々なことを高品質にこなす**（外部DNSサービス）

「大人として振る舞う」 ことを要求されるようになった

「DNSはもう限界」 と言われつつ^[*1]、**20年以上が経過した**

[*1] The DNS Today - Are we Overloading the Saddlebags on an Old Horse? – IETF 49
<<https://www.ietf.org/proceedings/49/slides/PLENARY-3/sld001.htm>>

3. 明日のDNSのカタチとは

このパートの内容

- 起こりつつある変化から今後起こりうる変化の兆しを捉え、明日のDNSのカタチについて考える
 - 起こりつつある変化
 - 今後起こりうる変化の兆し
 - 未来のDNSに望むこと
 - おわりに：明日のDNSのカタチとは

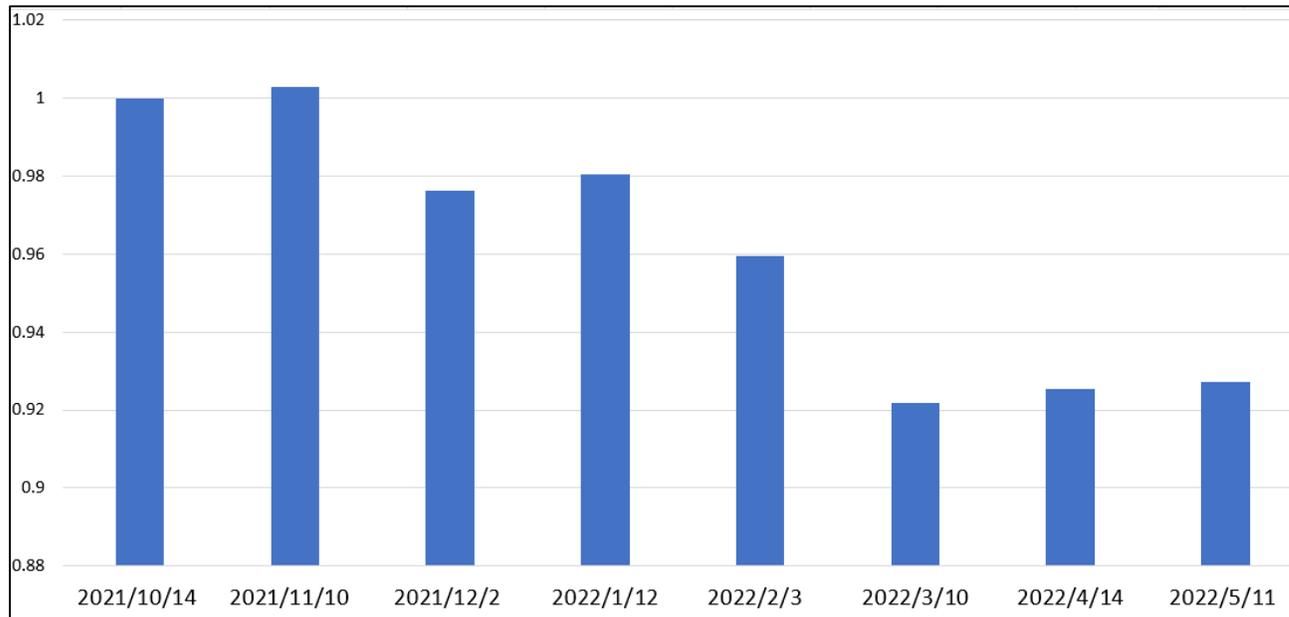
起こりつつある変化（HTTPSレコード）

- **HTTPSサービスに特化した、新しいリソースレコード**
- **HTTPSに関するさまざまなニーズを一度に実現**
 - ゾーン頂点の別名・Webサーバーの優先度設定・HTTPS接続情報の提供
- IETFにおける標準化作業は終了、RFC発行待ち
- RFC発行前であるが、**既に実装・対応が進んでいる**
 - Chrome・Firefox・Safariは**既に実装済み**
 - Safariは**デフォルトで有効**
 - CloudflareにWebサーバーと権威DNSサーバーの双方をホスティングすると、**HTTPSレコードが自動的に設定**

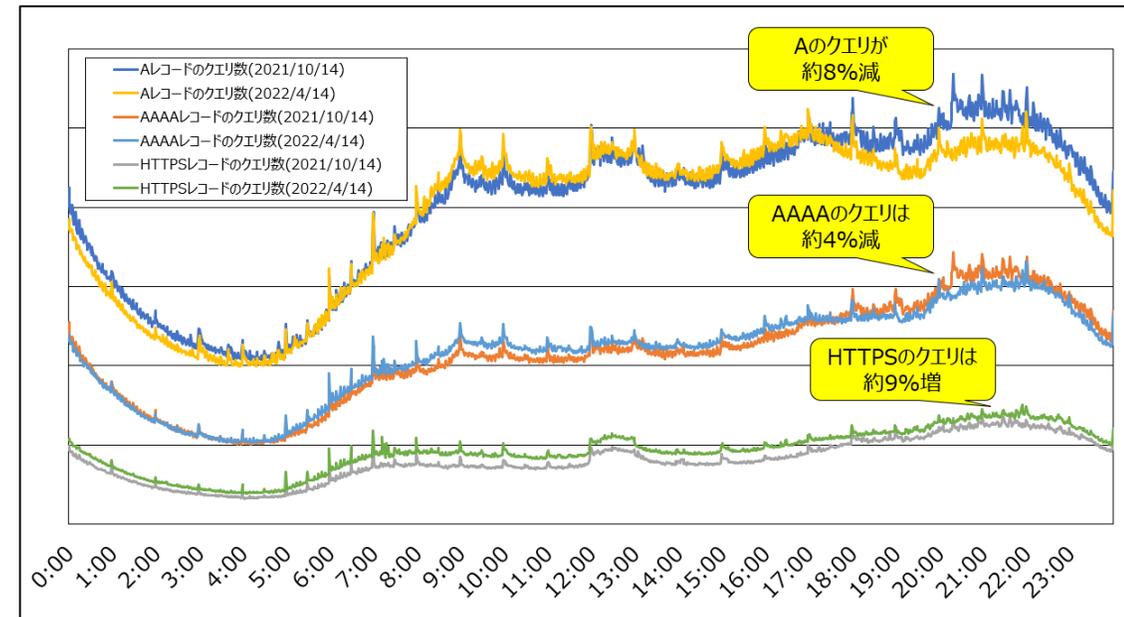
HTTPSレコードの普及状況

- ある大手ISPのフルリゾルバーにおけるクエリ数の変化
 - フルリゾルバーに到達するDNSのクエリ総数が**減少傾向**に

Special thanks to Ryota Kosaka @ NTT Communications



2021年10月～2022年5月のクエリ総数の推移



2021年10月と2022年4月のクエリ数の比較

グラフから推測されること

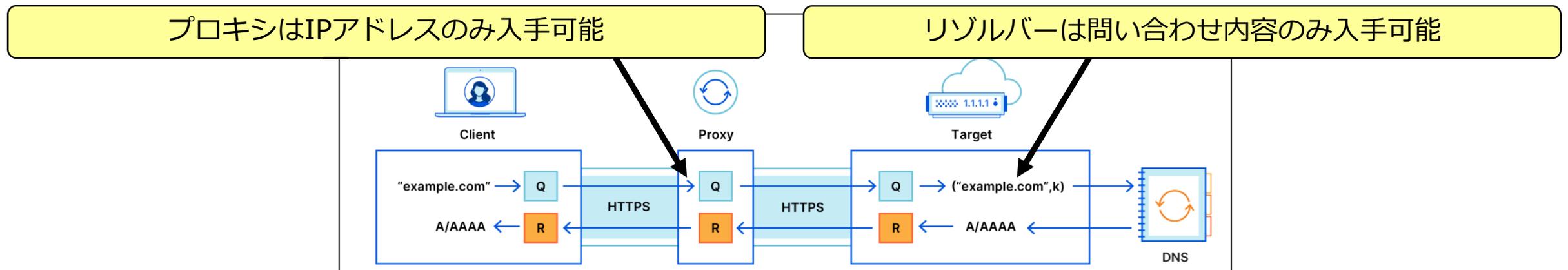
- **HTTPSレコードが使われ、効果を発揮し始めた**
 - **第一段階**：Webブラウザが対応し、クエリ数が**増える**
 - HTTPSレコードの後、A/AAAAレコードも問い合わせる
 - **第二段階**：権威DNSサーバーも対応し、クエリ数が**減る**
 - IPアドレスは**HTTPSレコードのipv6hint・ipv4hint**で入手

第一段階を過ぎ、**第二段階に入った可能性あり**

DNSを名前解決だけでなく、
HTTPSという**サービスの解決**にも使うようになった

起こりつつある変化（Oblivious DoH）

- **利用者のプライバシーを保護するための仕組み**
- IPアドレスとDNS問い合わせ内容を、**同時に入手されないようにする**
 - クライアントとリゾルバーの間にプロキシを追加
 - クライアントとリゾルバーがエンドツーエンドでデータを暗号化・復号
- Appleが**iCloud Private Relay**で採用
- **RFC 9230**として発行（2022年6月）



図の引用元：<<https://blog.cloudflare.com/oblivious-dns/>>

変化の理由

- HTTPSレコード・Oblivious DoHはいずれも、**インターネットのサービス形態・利用形態の変化**への対応と言える
 - HTTPSレコード：サービス形態の変化
 - Oblivious DoH：利用形態の変化
- 今後起こるであろう変化も、インターネットのサービス形態・利用形態の変化が鍵になると考えられる

インターネットに今後起こり得る変化は何か？

今後起こり得る変化の兆し

- 変化のヒント（キーワード）
 - 例：一対一の通信→一対多の通信→**多対多の通信**
 - 例：**移動体通信**の更なる強化（5G・6G）
- それらに伴う、**名前空間の位置づけ**の変化
 - 例：**情報指向ネットワーク（ICN）**
 - ユーザーはサーバーではなく、コンテンツ名を指定してコンテンツ取得を行う^[*1]

[*1]情報指向ネットワークがもたらす可能性と研究課題

<<https://www.nict.go.jp/publication/shuppan/kihou-journal/houkoku-vol61no2/K2015N-06-01.pdf>>

利用者が直接にはDNSを使わなくなる未来もあり得る

利用者が直接にはDNSを使わなくなる未来

- 利用者が直接にはDNSを使わなくなるのであれば、
「**覚えやすく使いやすい名前を提供する**」という、DNSのそもそもの目的が変わってくる可能性がある
- 目的の変化に対応した**新しいネーミングサービス**が開発され、広まるかも知れない
 - **TCPに対するQUIC**のような形
 - **さまざまなサービスとの連携**も
 - CDNサービスとの連携やHTTPSレコードは、その方向性の一つと言える

未来のDNSに望むこと

- 新しいネーミングサービスがもし開発されるとしたら、DNSのこれらの問題が解決されてほしい
 - **データの更新に冷たい**：データを更新したら、能動的に伝えたい
 - **運用ミスに冷たい**：うっかり公開したデータを取り消せてほしい
 - **切り替えがスムーズ**：「いつ切り替わります」とはっきり言いたい

いずれも、私が30年以上悩んできた問題
(他にもいろいろあるけど、特に何とかしたい)

おわりに：明日のDNSのカタチとは

- **明日のDNSは、まだDNSであろう**
 - 「もう限界」と言われつつ、20年以上が経過
- **しかし、今後インターネットのサービス形態・利用形態の変化に対応した新しいネーミングサービスが開発され、利用者はそれを使うようになるかもしれない**
- **利用者が直接使わなくなったとしても、インターネットを支える基盤技術としての、DNSの重要性は変わらない**

明日の、そして未来のインターネットを支えるため、一緒に頑張っていきましょう

最後までご視聴いただき
ありがとうございました！

jPRS

<<https://jprs.jp/tech/>>



[@JPRS_official](https://twitter.com/JPRS_official)



[JPRSofficial](https://www.facebook.com/JPRSofficial)



[JPRSpres](https://www.youtube.com/JPRSpres)