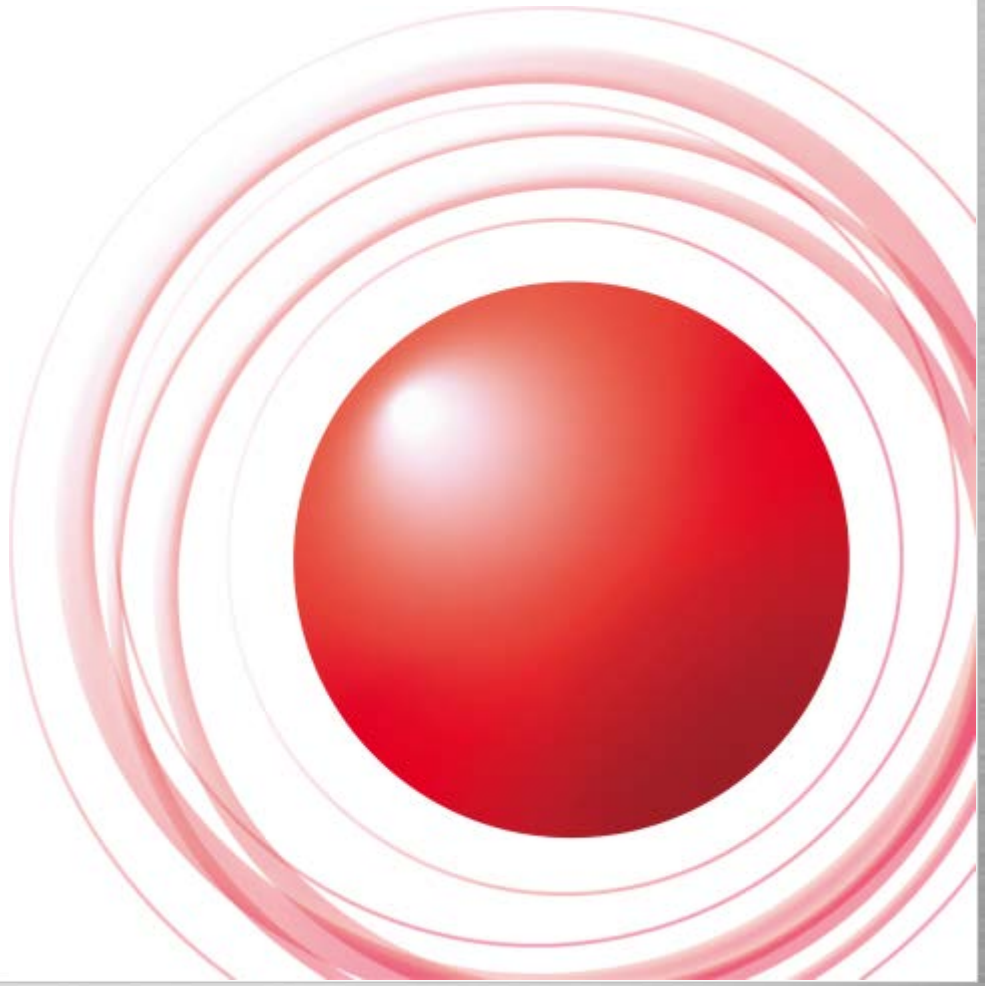
# IIJ Public DNSサービス（ベータ）のご案内

IIJ
Internet Initiative Japan



Ongoing Innovation

# IIJ Public DNSサービス（ベータ版）をリリースしました

## IIJ、「DNS over TLS」、「DNS over HTTPS」を利用したDNSの試験サービス「IIJ Public DNSサービス（ベータ版）」を提供開始

2019年5月8日

> このニュースのPDF版 [176KB]

株式会社インターネットイニシアティブ（IIJ、本社：東京都千代田区、代表取締役社長：勝 栄二郎、コード番号：3774 東証第一部）は、DNSサーバとの通信を暗号化する「DNS over TLS（DoT）」および「DNS over HTTPS （DoH）」を利用した「IIJ Public DNSサービス（ベータ版）」を、本日より無償公開いたします。本サービスはDNSキャッシュサーバの機能を試験サービスとして提供するもので、DoT/DoHに対応したブラウザ、端末にDoT ホスト名/DoH URLを設定することで、どなたでもご利用いただけます。なお、試験サービスの提供期間は2022年3月31日までを予定しています。

# IIJ Public DNSとは

**DNS over TLS(DoT), DNS over HTTPS(DoH)**
**だけに対応した、キャッシュDNSサービス**

**プライバシーにも配慮し、運用上、取得するデータの詳細、保存期間についても明記しています。**

**使い方については公式WEBへ**
**https://public.dns.iij.jp/**

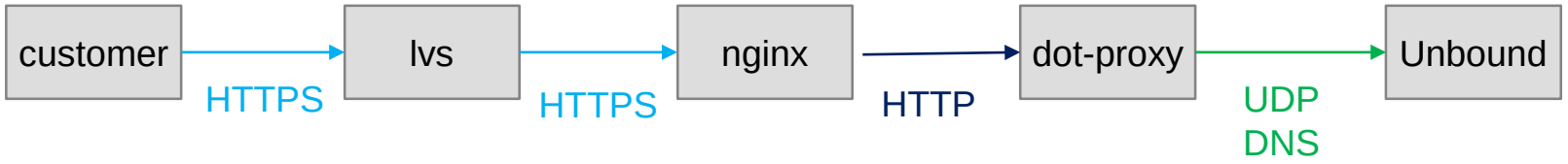
# 構成

# DoTの構成

- **UnboundがTLSを終端します。**
- **この構成を採用するために、UnboundにDoT関連のパッチを送っています。(1.9でmerge)**
  - TLS Session Ticket対応
  - cipher設定対応
- **LB側でTLSを解く構成に比べて、TLSを解ける台数を稼げる。**
- **処理能力が足りなくなったらアクセラレータを入れる予定**

# DoHの構成

- **UnboundはDoHに対応していません。**
  - Knot-resolverは間に合わず。
- **現在は、DoHのリクエストを変換するdot-proxyを通して実現しています。**
  - TLSの終端はnginxで行い、dot-proxyにhttpでプロキシ
  - dot-proxyでdns messageを作りUDP DNSでUnboundに問い合わせ
  - 結果をhttpにしてnginxに返し、nginxが暗号化してレスポンスを返す

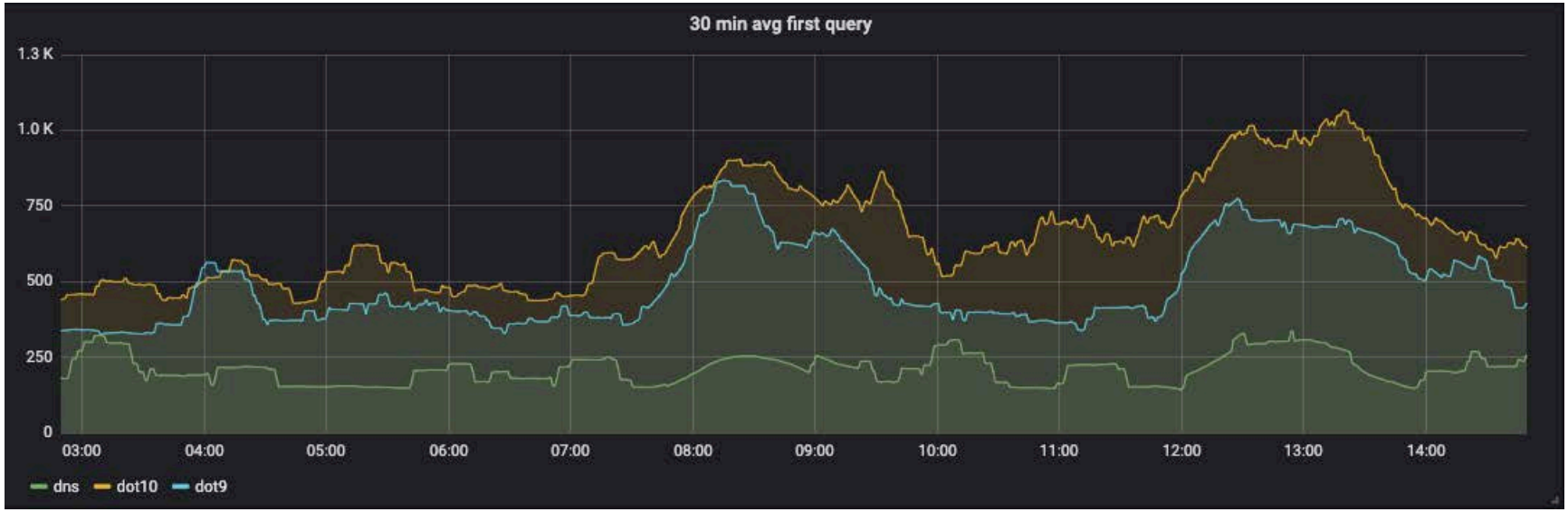


# おまけ

# レスポンスタイムを測定してます。。

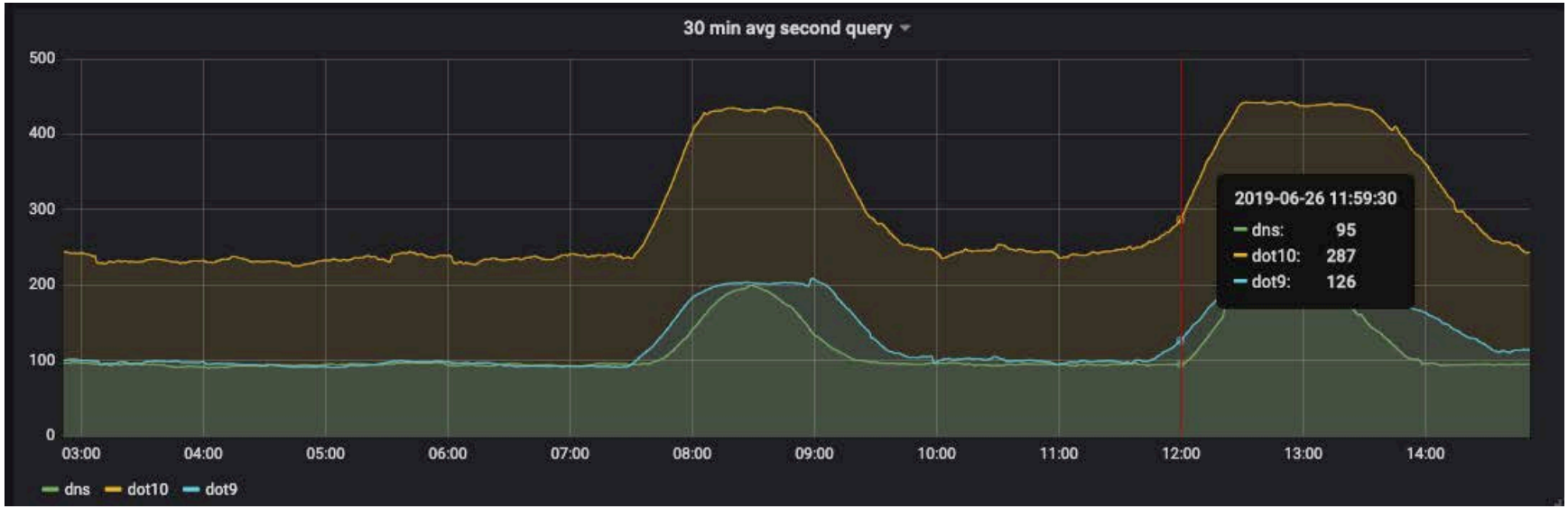
- 固定回線に導入するのは特に問題なさそうなのですが
- モバイル系で不具合報告が多発
- 検証用端末を使って、モバイル回線で６０秒おきに２回、レスポンスタイムを計っています

- １回目３０分平均したグラフがこんな感じ



# レスポンスタイムを測定してます。。

- ２回目３０分平均したグラフがこんな感じ




- DoTはTCP 接続が繋ぎっぱなしなので、SecondパケットはUDPと変わらないレスポンスタイムに
- DoHはTLS Session Ticketの効果でTLSハンドシェイクが短縮されるので
  半分のレスポンスタイムに