

QUIC(TLS 1.3)実装進捗

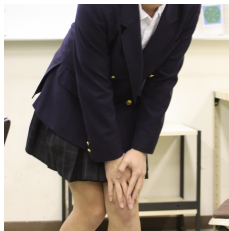
unasuke

RubyKaigi 2025 follow up

2025-08-30

自己紹介

- Name: うなすけ
- Work: フリーランス
- Kaigi on Rails 2025オーガナイザー (09/26-27 開催)
- GitHub <https://github.com/unasuke>
- Fediverse <https://mstdn.unasuke.com/@unasuke>
- X https://twitter.com/yu_suke1994
- <https://unasuke.com>



元ネタない勢(1人)

- 16:30 休憩
- 16:55 セッション4
 - (5分)「QUIC(TLS 1.3)実装進捗」 by うなすけ
 - (15分)「Namespaceその後」 by tagomoris ([元ネタ](#))
 - (15分)「Messaging Layer Security on Ruby 続き」 by sylph01 ([元ネタ](#))
 - (15分)「Unicode Normalization FormsのRuby実装について」 by ima1zumi ([元ネタ](#))
- 17:45 休憩

経緯

1. QUICプロトコルをRubyで実装したい
2. 一旦Python実装のRuby移植は不完全ながらできた(これがGrantでの成果)
3. より”Rubyらしい”コードになるように実装し直している
4. **QUICを実装するためにはTLS 1.3を実装しないといけない** ← ｲﾏｺｺ

ずっとTLS 1.3の実装してる

進捗

実際にご覧いただく

今のは何？

- `www.example.com` に対して (https) HTTP/1.1 でGET requestを飛ばしている
- TLS handshakeをする
- 返ってきた暗号化されたデータを解く
- 標準出力に表示しておしまい

取り組んでいたこと

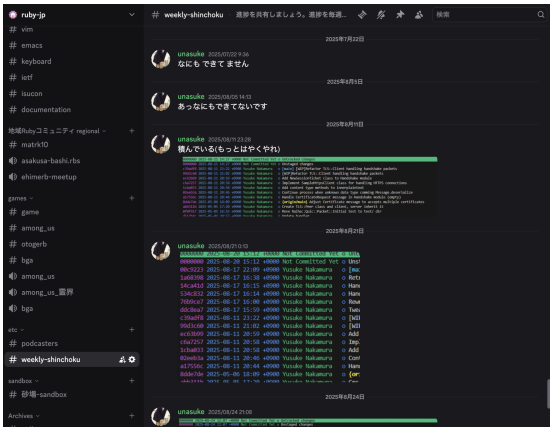
- Client側Handshake flowのリファクタ
- そもそもHTTPSでreq/resをするサンプルクライアントの実装
- 色々不足していたものたちの実装&リファクタ

取り組んでいたことlist

- [QUIC実装月報 2025年3月 | うなすけとあれこれ](#)
 - 進捗らしい進捗があるのはここだけかも
- [QUIC実装月報 2025年4月 | うなすけとあれこれ](#)
- [QUIC実装月報 2025年5月 | うなすけとあれこれ](#)
- [QUIC実装月報 2025年6月 | うなすけとあれこれ](#)
- [QUIC実装月報 2025年7月 | うなすけとあれこれ](#)

やっけたよ

ruby-jp discordの #weekly-shinchoku で垂れ流しています



実際にご覧いただく2

実際にご覧いただく

HELP ME

会場にお越しのTLS有識者の方

今後の展望

- 明日からまた開発中断します
 - Kaigi on Rails 2025のため……
- 10月から復活！
 - したい……