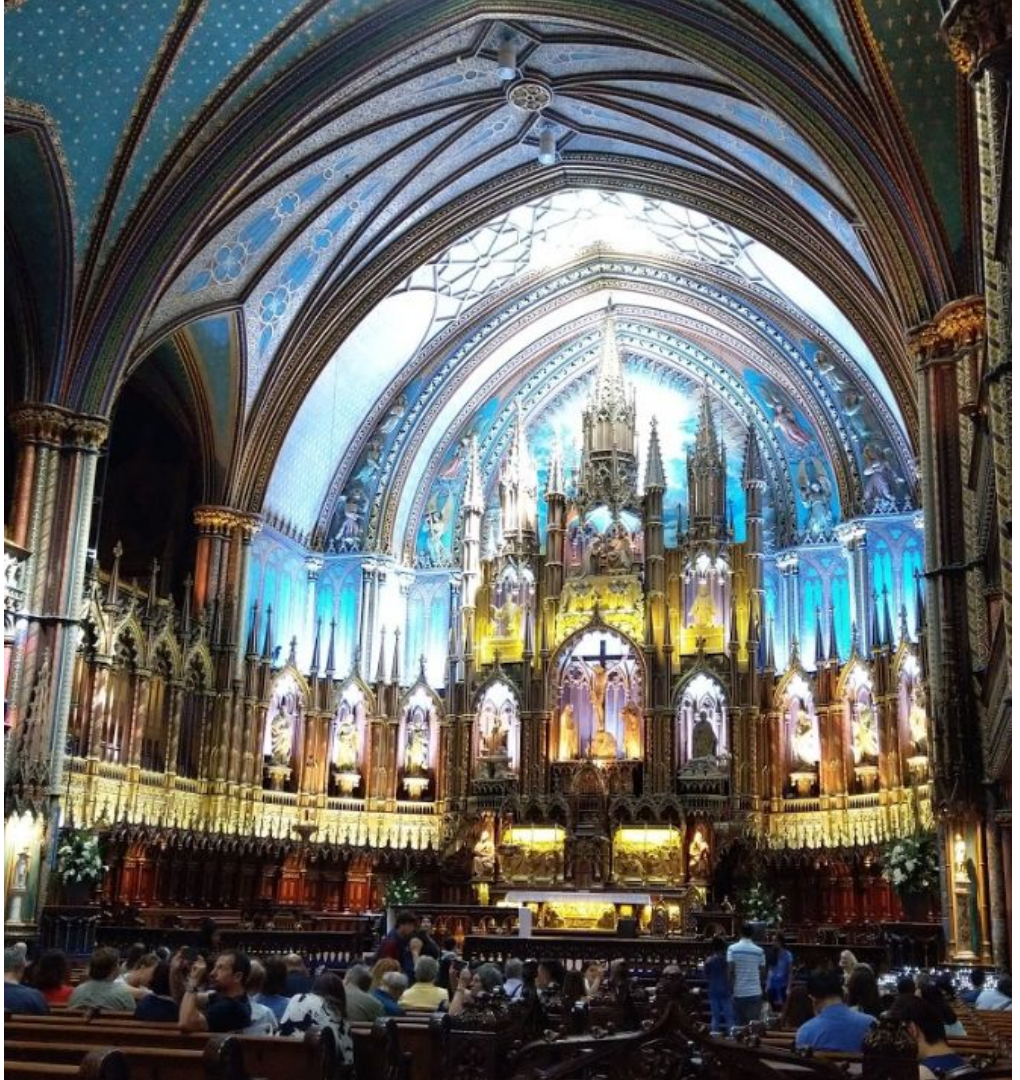
IETF 102 HTTP/QUIC 関連

後藤浩之 (グリー)



自己紹介

- 後藤 浩之 (グリー)
  - インフラ担当
- ISOC-JP インターネット標準化推進委員会
- 興味：Web, HTTP・QUIC関連

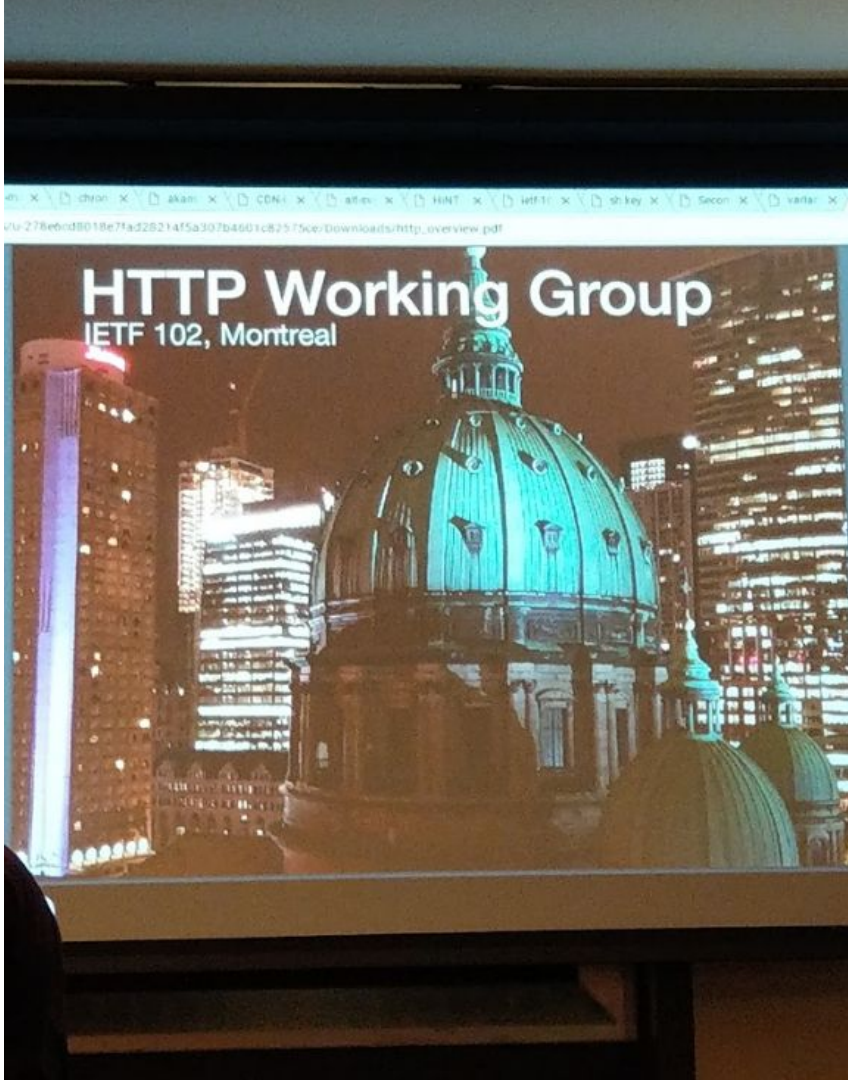
目次

- HTTP
  - HTTPwg
  - WPack
  - (SRV and HTTP)
- QUIC
  - QUICwg

HTTP関連

HTTP WG

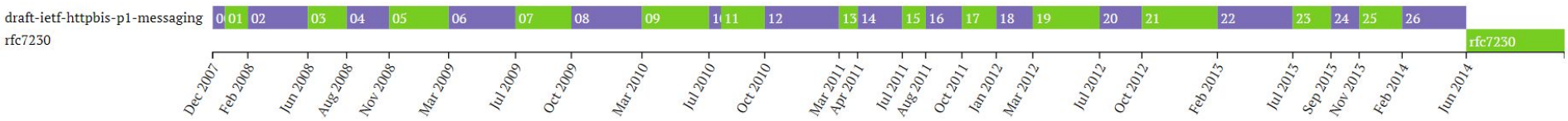
- 2セッション開催
- 引き続きのItemが多い (Issue整理)
  - HTTPTre
  - HTTP over QUIC
- New Item は少なめ
  - CDN Loop Prevention
  - Alt-Svc SNI and DNS ALTSVC
  - HTTP-initiated Network Tunnelling
-



HTTPtre (HTTP-Core)

- HTTP/1.1 (RFC 7230 ～ 7235) の再改定作業。
- RFC 723x のInternet-DraftがHTTPBisと呼ばれていたので、今度は”HTTPtre”。
- RFC2616 => RFC 723x には7年を要した。HTT/2やQUICなど、様々な変更やIssueがあるためメンテナンスを行う

(HTTPbis WGの名前はそのまま)



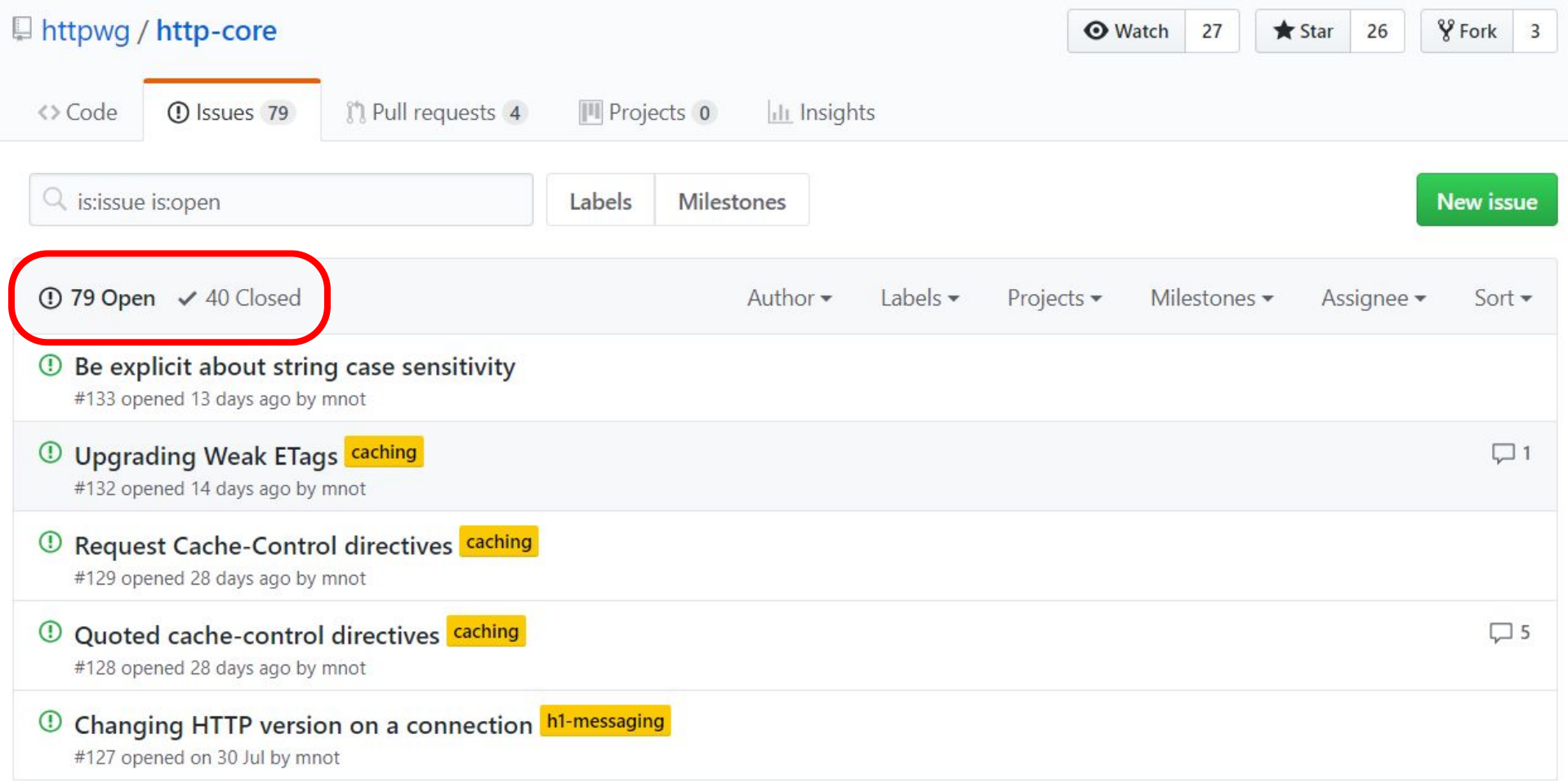
RFC723x の 7年

HTTPtre (HTTP-Core)

“HTTPのセマンティクス”と”HTTP/1.1 のシンタックス”を分離

RFC 7230 - Hypertext Transfer Protocol (HTTP/1.1): **Message Syntax and Routing**
RFC 7231 - Hypertext Transfer Protocol (HTTP/1.1): **Semantics and Content**
RFC 7232 - Hypertext Transfer Protocol (HTTP/1.1): **Conditional Requests**
RFC 7233 - Hypertext Transfer Protocol (HTTP/1.1): **Range Requests**
RFC 7234 - Hypertext Transfer Protocol (HTTP/1.1): **Caching**
RFC 7235 - Hypertext Transfer Protocol (HTTP/1.1): **Authentication**

draft-ietf-httpbis-semantics-02 - **HTTP Semantics**
draft-ietf-httpbis-cache-02 - **HTTP Caching**
draft-ietf-httpbis-messaging-02 - **HTTP/1.1 Messaging**



https://github.com/httpwg/http-core/issues

CDN Loop Prevention

攻撃者がCDNに悪意ある設定・リクエストを送信することで、永遠にHTTPリエクストをCDNでforwardさせ続ける攻撃手法がある。
(Forwarding-Loop Attacks in Content Delivery Networks)

ループを防ぐためにCDN-Loopヘッダを定義し、それを見ることでループを検知する。

```
CDN-Loop: FooCDN, barcdn; host="foo123.bar.cdn"
CDN-Loop: baz-cdn; abc="123"; def="456", anotherCDN
```

=> WG Adoption (https://tools.ietf.org/html/draft-cdn-loop-prevention-00)

Alt-Svc SNI and DNS ALTSVC (1/2)

alt-svcとは、Webサービスを別の別のプロトコル・サーバで提供できることをクライアントに通知する仕組み。

たとえば、example.comはexample.netのサーバでも提供できる事を示す例

```
Alt-Svc: h2="example.net:443";
```

このレスポンスヘッダを受け取ったブラウザはexample.netにつなぎに行く。このときのSNIは元のドメインの証明書(example.com)になる

Alt-Svc SNI and DNS ALTSVC (2/2)

Alt-SvcにSNIのフィールドを追加する。

```
Alt-Svc: h2="example.net:443";sni=example.net
```

TLS SNIはexample.comを使うが、HTTP/2コネクション確立後に
「CERTIFICATE_REQUEST」フレームを送信しexample.netの証明書を要求する

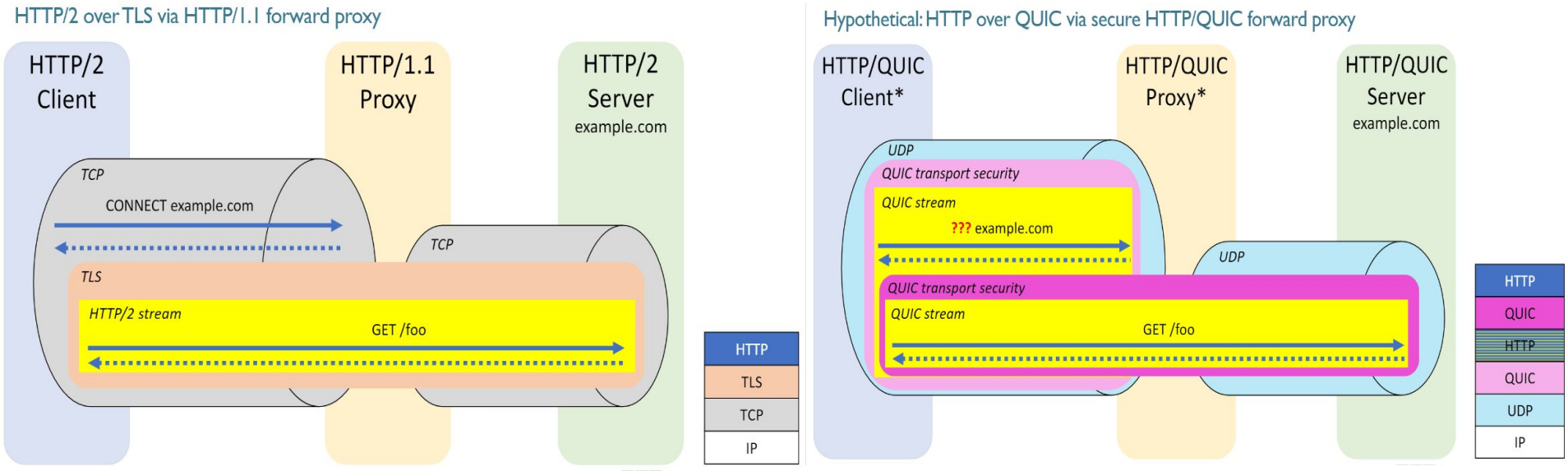
こうすることで、example.netへの接続要求であることが秘匿できる。

DNS ALTSVCでは、上記のalt-svc情報をDNSレコードで表現できるようになる。

＝＞TLS ESNIとの比較の議論などなど

HTTP-initiated Network Tunnelling

- QUIC(UDP)での、Proxyトンネリングの議論



wpack (Web Packaging)

- Webサイトを一つのファイルにまとめ再配送可能とする仕組み
  - オフラインでのWeb閲覧や、USBメモリによる受け渡しなどの用途
  - そのドメインのページを別のサーバから提供できる
- 2つの仕様からなる
  - Bundled HTTP Exchange: 複数のHTTPリクエスト・レスポンスを一つにする
  - Signed HTTP EXchange: 署名をし再配布可能にする
- これの仕組みによって、本来のURLとは別のところからそのURLからのレスポンスとして提供できるようになる
  - コンテンツの識別子とサーバの場所がURLで一つになっていたが、分離可能となる

wpack (Web Packaging) shide meeting

- IETF 102 でも Shide Meetingが実施される
- 主要なHTTPbisの人たちと予定が合わず、人はまばら
- 内容
  - ユースケースの確認
    - CDN
    - Service Workerとの連携
  - 進め方など
    - セキュリティ上の懸念
    - W3C/WhatWGと連携して勧めていく必要がある

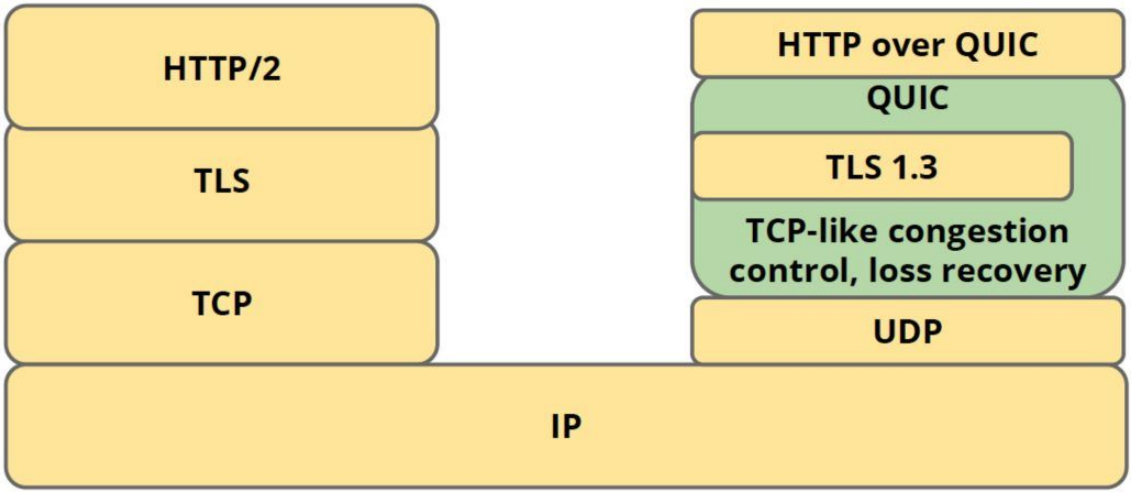
SRV and HTTP side meeting

- HTTPでのSRVの利用についての議論
- Use cases for SRV:
  - 1. Load balancing
  - 2. Service on alternate port
- HTTPではAlt-Svcを使ったりと、別の仕組みを使っている
- より良い方向性は？専用のレコード or Txtレコード?

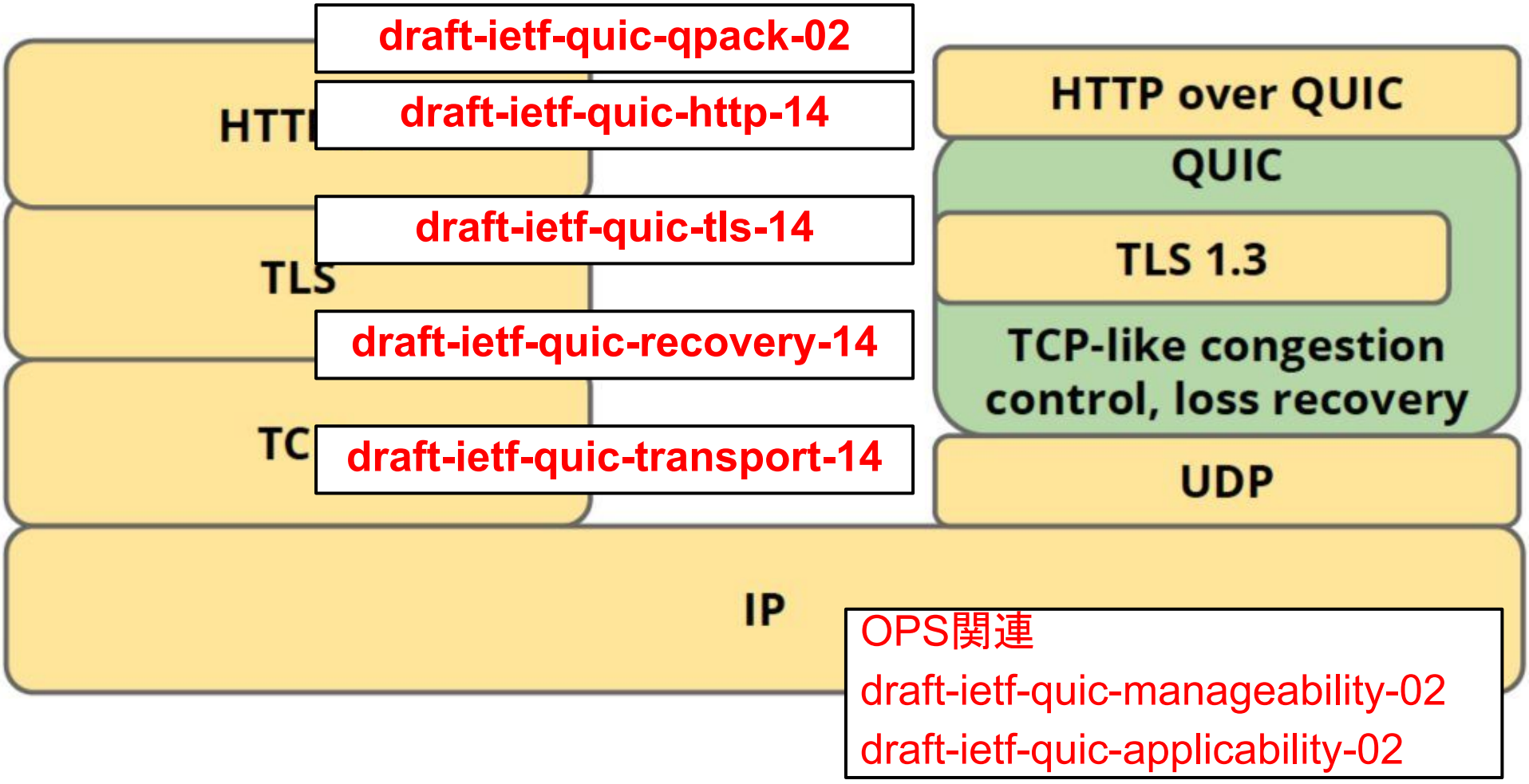
QUIC関連

QUICとは

QUICとは、Google社が考案したプロトコル
UDP上で動作し、TCPのような信頼性と、TLSのように暗号化された通信を提供する。上位プロトコルとして、HTTPを想定しているが限定はされない



引用 IETF98 QUIC Tutorial 14p
https://datatracker.ietf.org/meeting/98/materials/slides-98-edu-sessf-quic-tutorial


draft-ietf-quic-qpack-02
draft-ietf-quic-http-14
draft-ietf-quic-tls-14
draft-ietf-quic-recovery-14
draft-ietf-quic-transport-14
HTTP over QUIC
QUIC
TLS 1.3
TCP-like congestion control, loss recovery
UDP
IP
OPS関連
draft-ietf-quic-manageability-02
draft-ietf-quic-applicability-02

ハッカソン

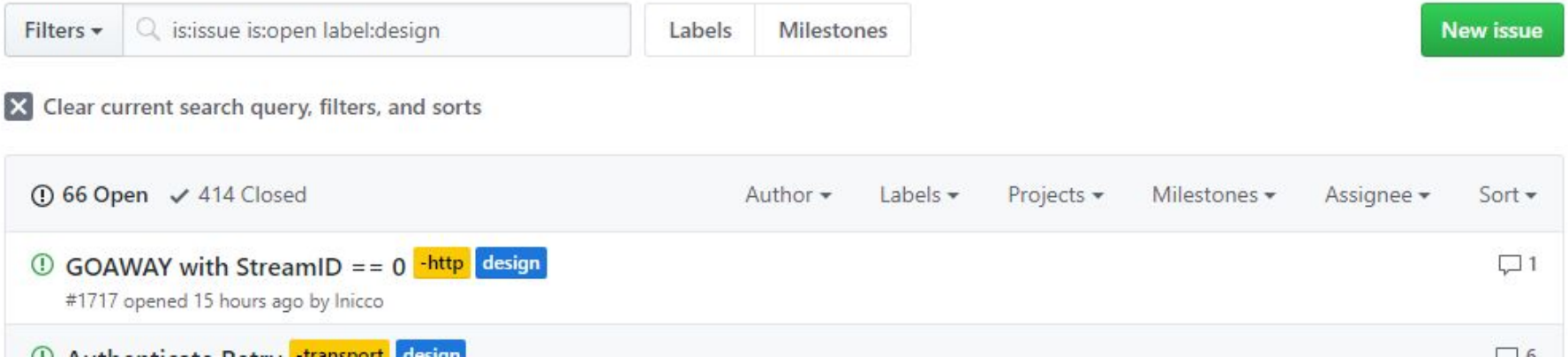
- 7th Implementation Draft

H: handshake
D: Stream Data
C: Connection Close

	Minq	Mozquic	Quicly	quant	ngtcp2	mvfst	picoQUIC	winquic	f5	ATS	Pandora	AppleQUIC	ngx_quic	!gquic	q
Minq	HDRZ		HD										HD		
Mozquic															
Quicly	HD		VHDRZ		VHDRZ								VHDR		
quant															
ngtcp2	HDC		VHDC		VHDCRZ								VHDC		
mvfst															
picoQUIC			VHDCRZ		VHDCRZ		VHDCRZS						VHDCR		
winquic			VHDCRZ		VHDCRZ		VHDCRZS	VHDCRZS		VHDCRZ			VHDCR		
f5															
ATS			VHDC		VHDC					VHDC			VHD		
Pandora															
AppleQUIC															
ngx_quic															
!gquic															

QUIC WG

- 1セッション開催
- やはり、大部屋開催
- 個人的な印象としては
  - 大きな変更は、いくつか入ったが落ち着いてきた => invariants
  - 細かい議論はまだまだたくさんある
  - V1にむけて鋭意策定中



QUIC WG

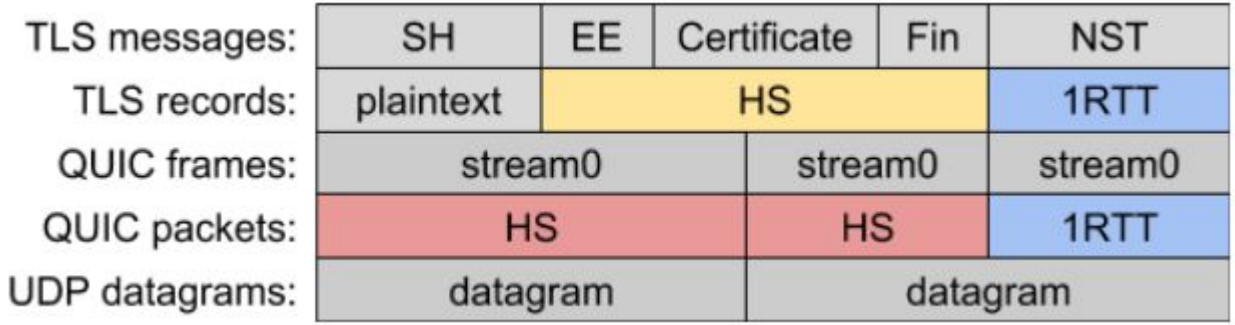
- 大きな変更
  - パケット番号の暗号化
  - **0 stream の再設計**: TLSハンドシェイク部分の変更
  - ECN in QUIC
- 議論
  - Connection IDs: Migration時のIDの記憶時間
  - Stateless Reset: 切断のループ問題
  - HTTP Priority: ゾンビストリーム
  - Spin Bit: 1bit 予約
  - QPACK

Stream 0 (1/2)

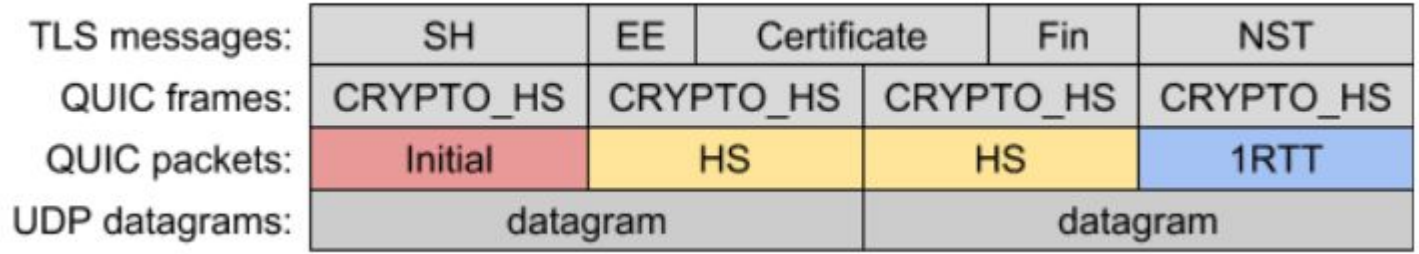
- QUICはTLS1.3のハンドシェイクをStream 0 で行っていた
  - Stream 0が非常に特殊扱いとなり、Stream 0の再送など条件などが複雑になっていた
- QUICとTLSスタックが密結合しており、レイヤリングを行いたいという議論などもあり
- IETF 101では QUIC over DTLSなどの提案もあったが、改めてデザインチームによって議論されることになった

Stream 0 (2/2)

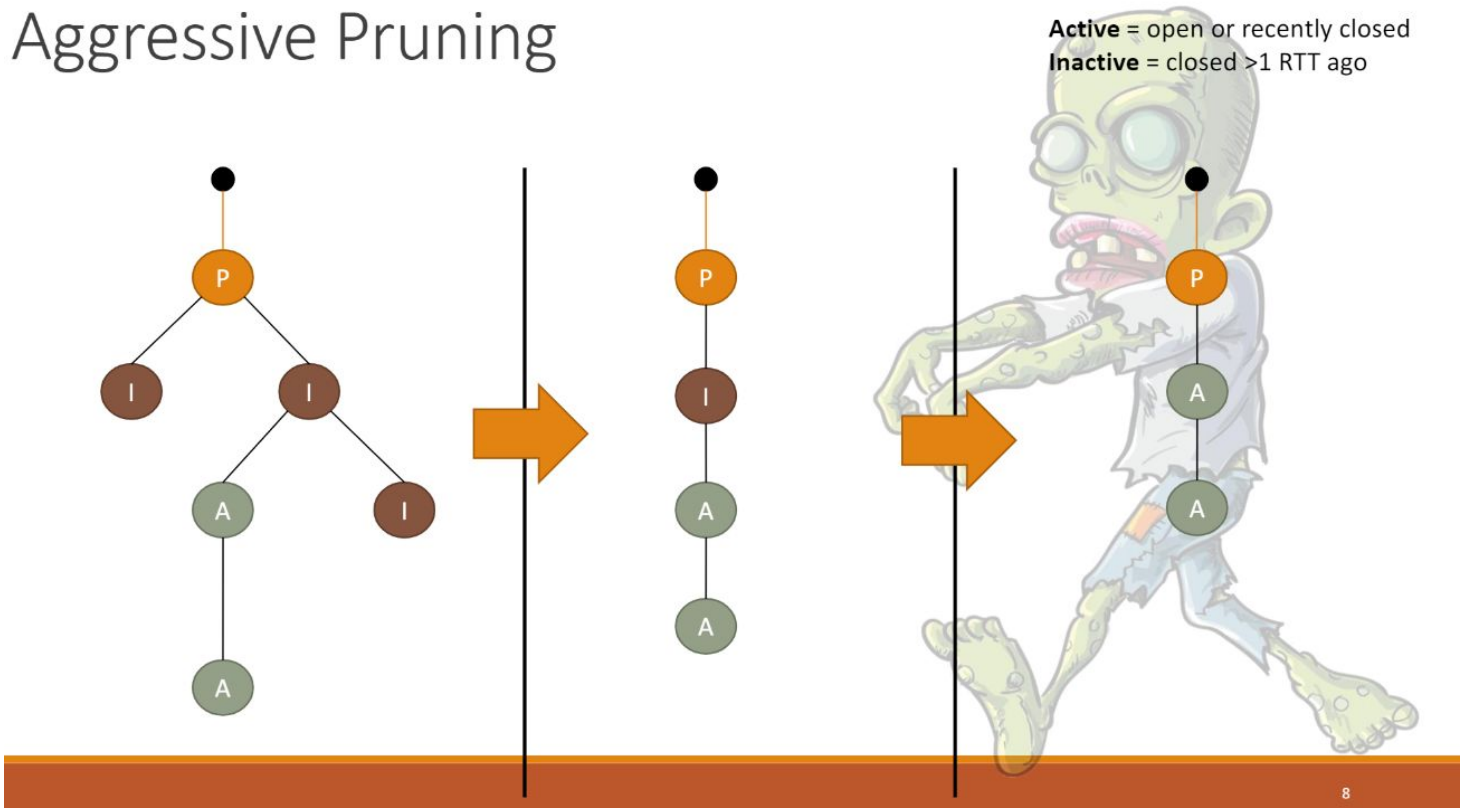
旧方式



新方式



HTTP Priority on QUIC



Other topic

- QUIC Version 44 and IETF QUIC
  - Chrome のGoogle QUICが IETF QUICへの移行をアナウンス
  - Google QUIC v44でInvariantsを対応
  - Chrome Canaryでオプション付きで有効に可能

https://groups.google.com/a/chromium.org/forum/#!msg/proto-quic/b6gZ18W5qn0/woUEYoBkDQAJ

今後

interim (September 17-18)

- 8th Implementation Draft

milestone

- Sep 2018 Version-Independent Properties of QUIC to IESG
- Nov 2018 Core Protocol document to IESG

おわりに

- HTTP
  - 拡張や新しい提案の議論もありつつ
  - メンテナンスを我慢強く進行中
- QUIC
  - 最初の頃に比べれば落ち着いてきた
  - ここの部分についてはまだまだ熱い議論がある