

# IETFにおけるトランスポート 関連技術の報告

2021年度

本多倫夫 [micchie@sfc.wide.ad.jp](mailto:micchie@sfc.wide.ad.jp)

西田佳史 [nishida@sfc.wide.ad.jp](mailto:nishida@sfc.wide.ad.jp)

慶應義塾大学SFC研究所

# 調査の概要

- 調査機関の名称
  - Internet Engineering Task Force (IETF)
- 調査対象テーマとその重要性
  - 国内機器ベンダにおける企業及び家庭向けネットワーク製品の開発や国内通信事業者のネットワーク運用にとって重要な、トランスポート層プロトコルおよびその拡張の標準化動向や技術トレンドの調査
- 調査の技術分野
  - トランスポート層技術に関連するトピック: TCP、ECN、QUIC、輻輳制御など
- 出席した会合
  - 111<sup>th</sup> IETF meeting (オンライン)
  - 112<sup>rd</sup> IETF meeting (オンライン)
- 調査者名
  - 西田佳史、本多倫夫

# IETFの概要

- インターネットにおける通信技術を標準化するために1986年に発足された団体
  - 組織や国としてではなく個人としての参加が前提。
  - Rough consensus and running code を基本とする意思決定ポリシー
  - メーリングリストで主に議論を進める。年3回全体ミーティングを開催する
- インターネットで運用される技術の標準化を行うため、Internet Protocol をベースに基本的にOSIネットワーク参照モデルにおける第三層以上の技術を扱う
- トピックごとにエリアという単位に分割される。（現在7エリア）
  - Applications and Real-Time Area (art), General Area (gen), Internet Area (int), Operations and Management Area (ops), Routing Area (rtg), Security Area (sec), **Transport (tsv)**
- 各エリアにおいてサブテーマ (特定のプロトコル等) 毎にワーキンググループ (WG) を作成し、標準化作業はそれぞれのWGで行われる。
  - WGの構成人数は各WGによって大きく異なる
- IRTF (Internet Research Task Force) という姉妹団体がある
  - IRTFは標準化は行わないが、IETFと並行しながら長期的視点でインターネット技術の議論を行う
  - 標準化に関連する学術論文の表彰なども行う
- 参加者は機器ベンダ、通信事業者、クラウド事業者、OS 開発者、アプリケーション開発者、大学教員/学生など多岐にわたる

# 調査対象テーマに関する国内外の状況

- 調査機関 (IETF) における活動
  - トラnsポートプロトコル技術の開発、標準化
    - TCPの問題点と修正案の標準化、高速化、セキュリティなど新機能の開発
    - 新しいプロトコルSCTP, QUICの開発、標準化
  - 輻輳制御技術の開発、標準化
    - Adaptive Queue Mechanismの開発、標準化(CoDel, PIE)
    - Explicit Congestion Notification(ECN)の開発、標準化
  - 帯域予約プロトコル (RSVP), Diffsurv など QoS 機構のメンテナンス、標準化
  - 上位層の HTTP や webrtc など web 関連技術と関係も深い
  - 輻輳制御アルゴリズム等技術の性質上、他のエリアと比べて参加者にアカデミア関係者が多い
- 関連する他機関の活動状況
  - W3C (web技術の標準化を行う、ただしプロトコル部分はIETF)
  - WIDE Project (TCP, SCTPの標準化に貢献 RFC5061, RFC6582, RFC6675, RFC7829)

# トランスポートエリア概説

- IETF における 7 エリアの 1 つ
  - OSI 4 層技術を中心とした技術の開発、標準化
  - 主なWG
    - TCPM ... TCPの比較的小規模な拡張と問題点の修正の標準化を行う
    - TSVWG ... TCPに特化しないトランスポート関連の技術やRSVPなどの標準化を行う
    - QUIC ... QUICプロトコルの開発、標準化を行う
    - TAPS .. トランスポートサービスの抽象化されたAPIの開発、標準化を行う
    - DTN .. Delay Tolerant Networking 技術の開発、標準化を行う
- IETF トランスポートエリアと関連の深い IRTF のRG
  - MAPRG .. プロトコルの挙動の解析やインターネットのトラフィック収集、解析に関する議論を行う
  - ICCRG .. インターネットにおける輻輳制御技術に関する議論を行う

# TSVWG ハイライト

- RFC 9065
  - トランスポートプロトコルヘッダが暗号化されていく (QUIC等) ことによる懸念事項を整理
    - ネットワークにおけるフローや再送パケットの特定などが困難になりネットワーク事業者にとってこれまでの方法におけるモニタリングができなくなる
- WG アイテム
  - ECN Encapsulation for Lower Layer Protocols
  - ECN for Tunnels that use Shim Headers
  - L4S (Low Latency Low Loss Scalable throughput)
  - UDP Options

# tcpm ハイライト

- 既存 RFC のマイナーアップデートが中心
- TCP HyStart++
  - スロースタートを遅延の増加に伴って早期に終了させる HyStart に異なる転送レート増加フェーズを追加
  - ジッター耐性を追加する技術に関する議論
- More Accurate ECN Feedback in TCP
  - データを含まない ACK パケットによるシグナリングの middlebox 耐性に関する議論
- TCP Silent Close
  - サーバーのクラッシュなどにより大量の FIN パケットがネットワークに送信される問題を解決する提案

# QUIC ハイライト

- Version negotiation
  - 互換性の保証対象をどうするか
  - RTT を消費せずにネゴシエーションするにはどうするか
- ロギング
  - スキーマのフォーマットに関する議論 (JSON 優勢)
- Ack frequency
  - Ack パケットの頻度をデータ送信側が指定できるようにするためのパケットフォーマットの議論

# MAPRG ハイライト

- IoT デバイスにおける TLS の普及状況に関する研究発表
  - IoT デバイスの数は 2025 年までに 750 億個になると試算
  - TLS 1.2 は殆どのデバイスで使われているが TLS 1.3 や近代的な暗号化スイートの利用は限定的
  - 期限切れのサーティフィケートの利用も多い

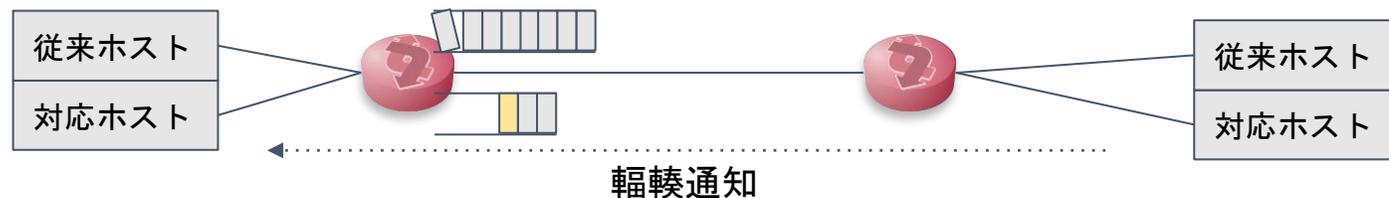
# 総括

- 111, 112 回会合におけるトランスポート関連技術のトレンド
  - 引き続き QUIC, L4S などが活発ではあったもののオンラインの長期化によりやや議論の進行が遅い印象

# Backup

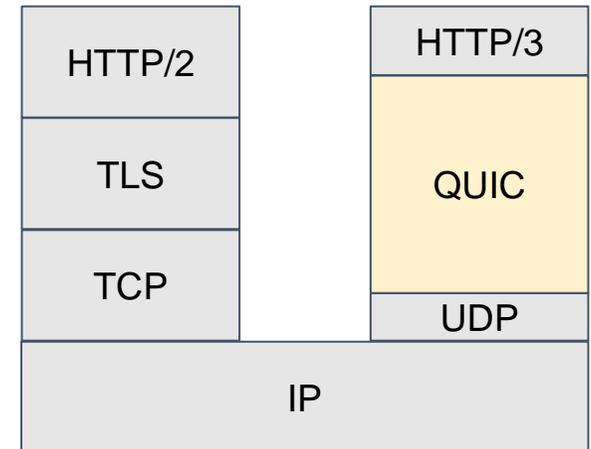
# L4S

- L4S (Low Latency, Low Loss and Scalable throughput)
  - 従来の best-effort 型のサービスから対応ホストを切り離してサービスを実現を目指す
    - L4S 対応ホストの packets が従来のインターネットのキューに入らないように (遅延が増大しないように) する
  - ルータは ECN ビットの一部を利用して対応ホストかどうか検知
  - 対応ホストと従来ホストからの packets を別のキューに入れる (dual queues)
  - 対応ホストは ECN マーキングベースの輻輳制御を用いて柔軟で正確な輻輳制御を行う



# QUIC

- TCP と TLS を置き換えるトランスポートプロトコル
- HTTPでの利用を強く意識
- UDP上で動作
  - NATP や firewall などの Middlebox への対処
- TCP+TLSよりも低遅延な通信を実現
  - Zero RTT handshake が可能
- ほぼ全通信を暗号化
- TCPの様々な問題点に対する対策を取り入れた設計
- Apple, Fastly, Facebook, Microsoft, Google, Mozilla 等で実装が進んでいる
- QUICを利用する HTTP の新バージョンは、HTTP/3 として開発が進められている。(HTTP/2の開発も継続)



IETF で標準化が進められている QUIC は Google がすでにインターネット上で使用している QUIC とは別物

# Middlebox

- インターネットはルータがレイヤ3 (IPv4, IPv6) の情報を元のみパケットを転送されるように設計されてきたが、現実のインターネットでは多くの Firewall や NAT、プロキシ等レイヤ4以上の情報を元にパケットに変更を加えたり転送先を決定したりする middlebox と呼ばれる機器が多く存在する
- middlebox の動作はとても複雑で誰も把握していないレベルのものもあるため\*, トランスポート技術の標準化にはかならずこの問題がついてまわる

\* Is it still Possible to Extend TCP? M. Honda, Y. Nishida et al, ACM IMC'11

