IETF98報告会
QUIC WG調査報告

株式会社レピダム
岡田 耕司
2017/05/12

Copyright © 2004-2017 Lepidum Co. Ltd. All rights reserved.

自己紹介

- 2013年 レピダム入社
  - 主にネットワーク関連の研究開発プロジェクトでPM・エンジニアを担当

Copyright © 2004-2017 Lepidum Co. Ltd. All rights reserved.

QUIC WG概要

- WGの目的
  - TCP HoL blocking問題を解決するUDPベースのデータ転送メカニズムの標準化
- 活動概要
  - IETF 97以降Tokyo interimを経て、かなり早いペースで標準化が進んでいる
    - HTTP/2の資産を活用しつつ、QUICの独自色も出始めている
  - コアプロトコルについては大規模な改変が継続中
- 雰囲気
  - 会期に先立って行われたQUICチュートリアルでは、プレナリ部屋が超満員
  - WGミーティングでも活発に議論が進む

Copyright © 2004-2017 Lepidum Co. Ltd. All rights reserved.

QUIC WG IETF98アジェンダ

- QUIC Applicability and Manageability Statement
- Working Group Drafts
  - Transport
  - TLS
  - Recovery
  - HTTP
- Open Issues
  - 167 - Hash for unencrypted packets
  - 45 - Handshake protocol selection
  - 61 - Silent close
  - 391 - Packet number echo with variable-length numbering

Copyright © 2004-2017 Lepidum Co. Ltd. All rights reserved.

QUIC Applicability and Manageability Statement

- 以下2ドキュメントをWGドラフトとして採用
  - draft-kuehlewind-quic-applicability-00
    - QUICアプリケーション実装者へのガイダンス
  - draft-kuehlewind-quic-manageability-00
    - ネットワーク運用上のガイダンス

Copyright © 2004-2017 Lepidum Co. Ltd. All rights reserved.

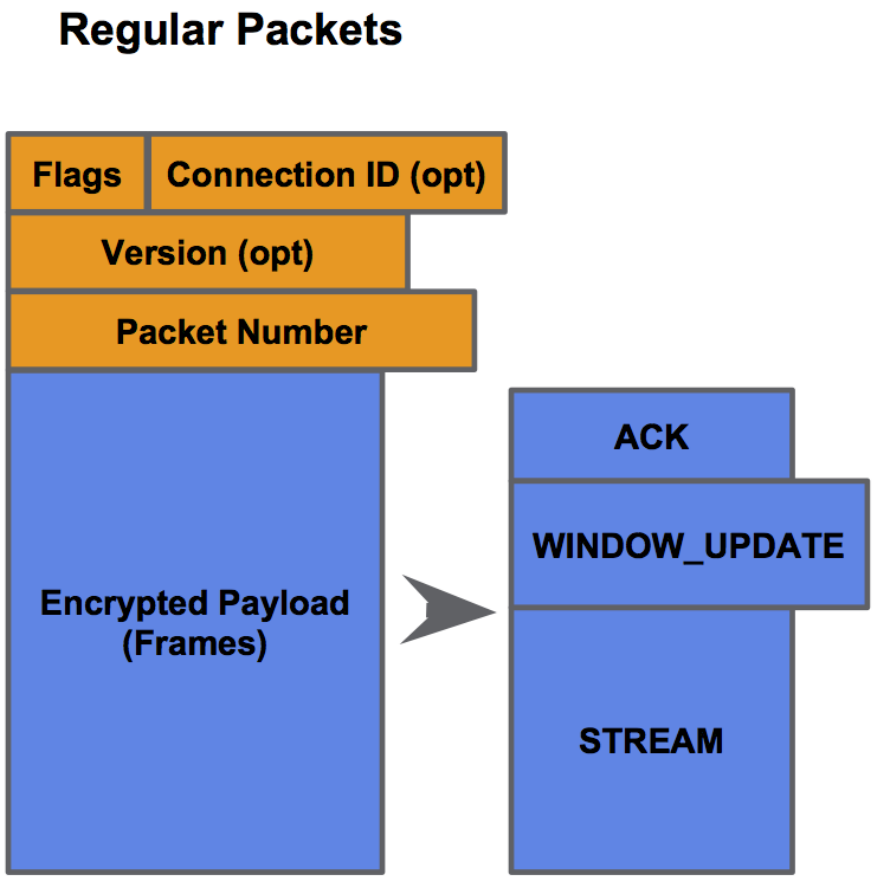
Transport

draft-ietf-quic-transport-02

- QUICプロトコルのコア部分に関する文書
  - パケット/フレームフォーマット
  - コネクション管理
  - 多重化
  - 等
- IETF 98における主要な変更点
  - コネクションIDネゴシエーション
    - サーバが最終的にクライアントが用いるコネクションIDを決定
  - パケットフォーマット変更
    - long header/short headerに分割
  - PMTUDの採用
  - initial packetsのサイズはTLSハンドシェイクメッセージを格納するのに十分な大きさに(>=1280 bytes)
  - フレームフォーマット調整

Copyright © 2004-2017 Lepidum Co. Ltd. All rights reserved.

-01 QUICパケットフォーマット

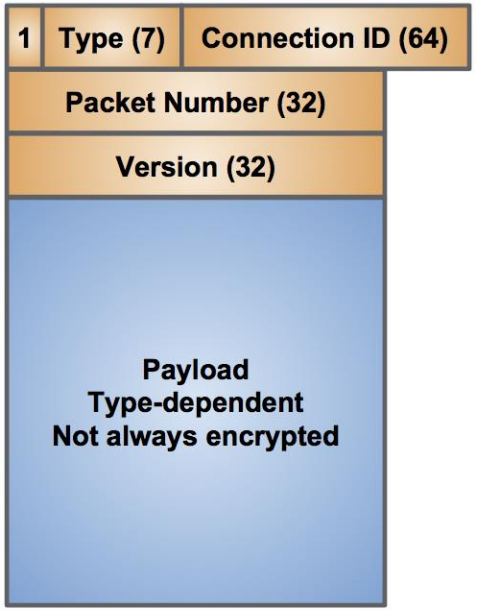


フラグ
* 0x01 = VERSION
* 0x02 = PUBLIC_RESET
* 0x04 = KEY_PHASE
* 0x08 = CONNECTION_ID
* 0x30 = PACKET_NUMBER_SIZE
* 0x40 = MULTIPATH
* 0x80 = unused

Copyright © 2004-2017 Lepidum Co. Ltd. All rights reserved.

long headerフォーマット

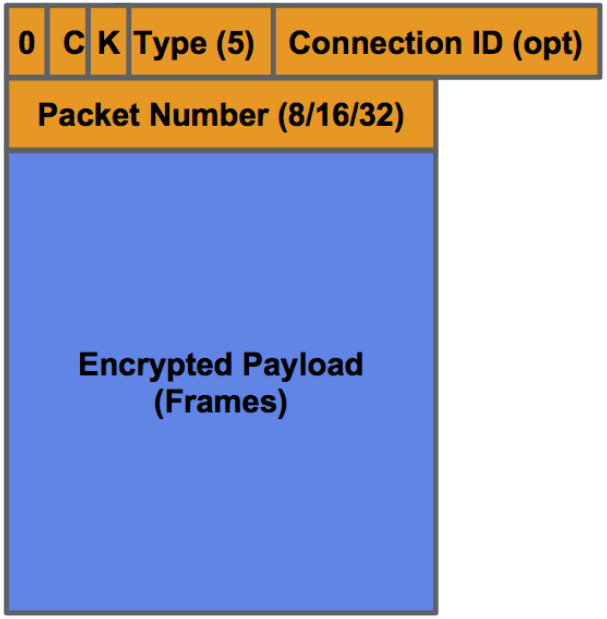
- 用途
  - バージョンネゴシエーションと1-RTT keyの交換が終わるまで使用
- 特徴
  - Connection IDフィールド、Versionフィールドは必須



Type	Name
01	Version Negotiation
02	Client Cleartext
03	Non-Final Server Cleartext
04	Final Server Cleartext
05	0-RTT Encrypted
06	1-RTT Encrypted (key phase 0)
07	1-RTT Encrypted (key phase 1)
08	Public Reset

short headerフォーマット

- 用途
  - バージョンネゴシエーションと1-RTT key確立完了後に使用
- 特徴
  - Connection IDフィールドはOptional
  - Versionフィールドを持たない



Type	Packet Number Size
01	1 octet
02	2 octets
03	4 octets

フラグ
- C: Connection ID
- K: Key phase

Connection ID長に関する議論

- Connection ID長として64bitは短すぎる？
  - パケットヘッダの最後尾にconnection IDフィールドを移しては？
  - 拡大したいときに拡大するのが楽になる・・・が
  - 現在のパケットヘッダフォーマットに変更を加えると、short header/long headerでパケットヘッダフォーマットの整合性が取れなくなる
  - ハードウェアにとってはconnection IDの位置は共通であることが望ましい

- QUIC WGとしてConnection ID長が64ビットでは短いことは認識している
  - 明確な問題が発生するまでは64bitのままとする、とされた
  - 極力オーバーヘッドを小さくする、というポリシに則っていると思われる

Copyright © 2004-2017 Lepidum Co. Ltd. All rights reserved.

QUIC TLS

- 特徴
  - 暗号化層(TLS)のハンドシェイクおよびパケット暗号化のための鍵スケジューリングを定義
- 変更点
  - ハンドシェイクはすべてunencryptedに
  - AEADのassociated dataにQUICパケットヘッダを追加

Copyright © 2004-2017 Lepidum Co. Ltd. All rights reserved.

Recovery

- 特徴
  - ロスリカバリや輻輳制御について定義
- 変更点
  - 時間ベースでのロス検知
    - RTOタイマー等
  - RTT計算の定義
    - smooth RTTベース
  - ハンドシェイクパケットのロスリカバリについての言及
    - early packetsに対するタイムアウト値計算等
  - NewRenoに関する記述を追加(まだスケルトン)
    - 以前のデフォルト輻輳制御アルゴリズムであるCubicに関する記述を削除

Copyright © 2004-2017 Lepidum Co. Ltd. All rights reserved.

HTTP

- 特徴
  - QUICプロトコル上にHTTP/2をマッピングする仕様について定義
- 変更点
  - ALPN, Alt-Svcに関する修正
  - SETTINGSフレームに関する修正
  - HTTP/2の拡張メッセージをポーティングする際のガイダンスを追加
- 関連
  - QUIC固有のヘッダ圧縮(QPACK, individual)

Copyright © 2004-2017 Lepidum Co. Ltd. All rights reserved.

Open issues(1/2)

- unencrypted packetsのハッシュ
  - 壊れたパケットを検知して捨てるのに、TCPチェックサムよりいい方法はないか
  - FNV-1aに決定
- Handshake protocol selection
  - 通信開始時にどのようにハンドシェイクプロトコルを知るのか？
  - 「QUICバージョンで固定値」「TLSに任せる」等
  - コンセンサスなし

Copyright © 2004-2017 Lepidum Co. Ltd. All rights reserved.

Open issues(2/2)

- Silent close
  - 明示的に閉じられなかった接続をどのように扱うか
  - ミドルボックスへの影響等を議論
- Packet number echo with variable-length numbering
  - ネットワークサイドでのRTT計測手法

Copyright © 2004-2017 Lepidum Co. Ltd. All rights reserved.