Web 関連

グリー株式会社 後藤

2015/12/8 IETF 94 報告会

自己紹介

- 後藤
- グリー株式会社
  - インフラエンジニア
  - 主に運用業務
- ISOC-JP Program commitee
- 今回 IETF 初参加
- 個人活動
  - HTTP2 Study
  - HTTP2 関連で書籍レビュー・寄稿

目次

Web関連

- HTTPbis WG
- WebPush
- QUIC 関連

その他

- ISS

HTTPbis WG

HTTPbis WG

- HTTPに関する仕様を議論
- HTTP/2 が標準化され、一段落した
- WGとしては、今後もHTTP(セマンティクス, HTTP/2)の拡張について議論

HTTPbis WG

Specification Status

- [The ALPN Header Field] : RFC7639
- [Client Initiated Content Encoding] : Editor Queue -> RFC 7694
- [An HTTP Status Code to Report Legal] : WGLC -> IESG Evaluation

alt-svc

オリジンのリソースを別のサーバ(IP),ポート,プロトコルで提供出来るようにする仕様。サーバからalternative serviceを通知して、クライアントがつなぎ直す仕組み。

- Security for spoofed certs(#98)
  - certificate-pinningの検証の追記
- using alt svc on localhost (#89) :close
- alt-svc vs the ability to convey the scheme inside the protocol(92)
  - セキュリティ上の混乱がおこりうる
  - HTTP/1 のようなプロトコルの中にscheme(http?https)を持たないプロトコルのリスクを追記する

https://github.com/httpwg/http-extensions

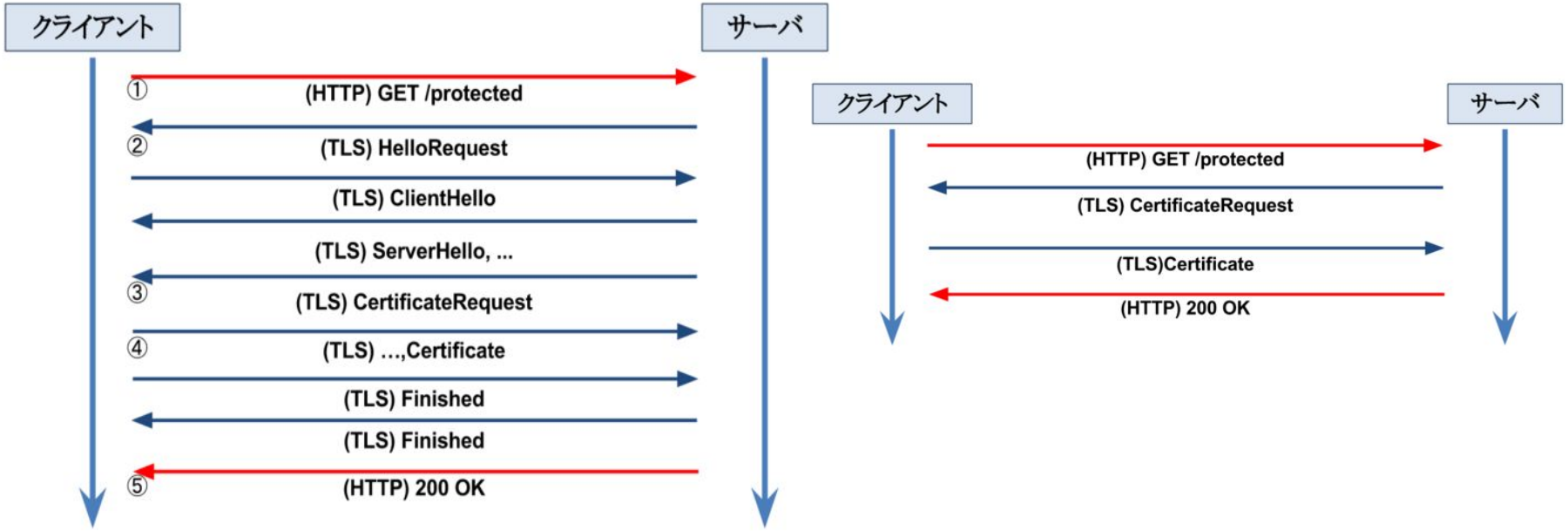
HTTPbis WG

Client Authentication

HTTP/2ではTLS Renegotiationが禁止されている。

TLS Handshakeが終わった後に、改てクライアント証明書を要求する場合の議論。

HTTP/1.1では、どのHTTPリクエストがrenagotiaon(TLS 1.2)の契機になったか分かったが、HTTP/2ではリクエストが多重化されているため、分からなくなる。
TLS1.2 及びTLS1.3でHTTP/2のストリームと、TLSのクライアント証明書を要求メッセージを紐付けるための拡張。



TLS 1.2　　TLS 1.3

HTTP/2 にWAITING_FOR_AUTHフレームを追加(この中にcontext_idを入れる)し、サーバ側が証明書が必要になったストリームでこのフレームを送信する。TLSのメッセージで、証明書を要求するメッセージで、このcontext_idを送信する。

引用 http://d.hatena.ne.jp/ASnoKaze/20151023/1445614131

HTTPbis WG

Push-Policy

HTTP/2 でストリーム毎にPushを制御するために、HTTPヘッダでクライアントの望むPush Policyをサーバに伝えられるようにする拡張

ServerがよりClientの状態に合わせてPushを行える事はいいことだが、まだ議論が必要。フィードバックが欲しい。

Cookie

Cookieセキュリティを向上するための3つの仕様。それぞれ、

- Leave Secure Cookies Alone :Secure Origin以外からSecure 属性を付与できないようにする
- First-Party Cookies: First-Party only 属性を付与し、first-partyへのリクエスト時のみcookie付与
- Cookie Prefixes: 属性をCookie名のpreffixに付与する

議論を継続

HTTPbis WG

Origin Frame

HTTP/2では一つのコネクション上で複数オリジンのリクエスト・レスポンスが行える。サーバが権威を持つOriginをクライアントに通知する拡張フレームの定義。

DNSに問い合せれば可能と言う話も出たが、実装者には好意的

The Key HTTP Response Header Field

HTTPレスポンスをキャッシュするための”キー”、Varyと違い 知識を必要とする。
「Key:cookie;param=_sess;param=ID」
=> draftをブラッシュアップして、実装を目指す

WebPush WG

WebPush WG

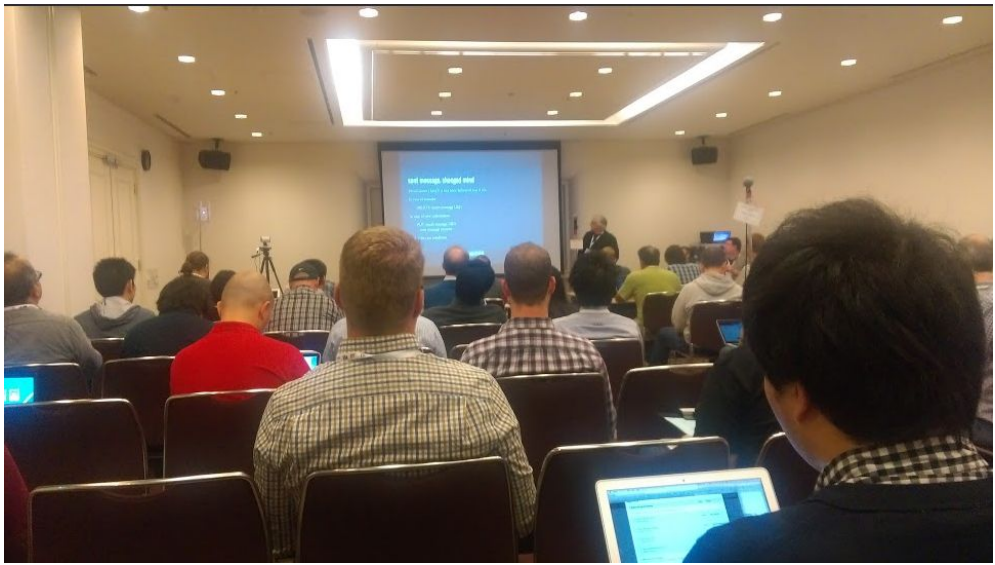
Webベース(HTTP)の通知PUSHの仕組みを検討するWG

まだまだメインとなる “draft-ietf-webpush-protocol-02 ” のコアスペックの議論を行っている。

WG item

- draft-ietf-webpush-protocol-02
- draft-ietf-webpush-encryption-01

https://github.com/webpush-wg



Web-Based Push Notifications (webpush)

draft-ietf-webpush-protocol-02

(UserAgent) < ----- > (Push Service) < ------ > (Application Server)

- Subscription Sets #53 : 複数のSubscriptionをセットとして扱えるようにする。
- Push Message Replacement #62 : Pushしたメッセージを変更する。PUT メソッド
- Negative Acknowledgements #12 : メッセージがExpireしてたおきのresponse status => 410
- Acknowledgement-Data #57 :
  UserAgentがPushメッセージを受領したことを Application Serverに

draft-chiussi-webpush-subscription-less-framework-01

- Use Case
  - 緊急信号、プライバシー保護
- Web Push Subscription Authority
  - 信頼されたAuthorityからPushを行う
  - DisvoveryやTrustについては今後議論を行う

QUIC 関連

QUIC 関連

Googleの提案・実装してるHTTP/2をUDP上で転送するトランスポートプロトコル。
TCP(信頼性・輻輳制御)・TLS(暗号化)相当の機能を有する。

前回のIETF93ではBoFが開かれたが今回は、BoFは開かれなかった。i-dは出ているが進捗はない。
開発者MLではTLS1.3の標準化を待って、標準化を進めるという話があった。

WebというコンテキストでQUICの議論はなかったが、トランスポートで報告あり

- HOPS RG(How Ossified is the Protocol Stack? Research Group)
  - Comparing TCP and UDP(QUIC) packet reordering
- TCPM (TCP Maintenance and Minor Extensions)
  - CUBIC fix in QUIC and Linux-TCP

QUIC 関連

hops: Comparing TCP and UDP(QUIC) packet reordering

- TCPのビデオトラフィックでは、7%の接続で3パケット分のreordering が発生
- QUICでのLoss Recovery Algorithmsの紹介
  - 3パケット分のreordering でFACKを送信
  - a time-based fast loss detection algorithm

  → spurious retransmitsを50%, 全体のretransmitを1~2%削減

tcpm: CUBIC fix in QUIC and Linux-TCP

- CUBICを再実装し、Linuxの実装にバグを見つけた
- Cubic is a complex beast
- Running in userspace helps

ISS Bof

ISS Bof

Internet Storage Sync Problem Statement

- Dropbox, Google Drive, One Driveのようないわゆる**Storage**サービス
- ユーザは各種クライアントソフトをインストールする必要がある
- Storage間のSyncが出来無い
- Standard API / Standard Syncプロトコルが無い
- 既存のStorageサービスの測定 => 小さいファイルだと非効率的

議論

= > どこまでをターゲットにするか。メタデータや構造の管理、ファイル転送プロトコル

= > 暗号化と重複削除

引き続きMLで議論(+on github https://github.com/labkode/Internet-Storage-Sync)

まとめ

HTTPBis
- **引き続きHTTPの拡張仕様の議論**
- **HTTP/2 でのClient認証、Pushの改善**

WebPush
- **Core Specの議論**
- subscription-less-framework の提案

QUIC
- **TLS1.3待ち、トランスポートとしてのフィードバック**

ISS Bof
- **Storage SyncのProblem statement**