IETF動向②ウェブ技術とHTTPプロトコルの動向

清水 一貴／木原 朴／林 達也　株式会社レピダム

加速するウェブブラウザーの革新とプロトコルの変化
スマートフォンの普及でHTTP通信の多重化や効率化へ

全体の動向

IETFを含んだウェブ関連技術の動向として、最近まではサーバーとクライアント間の双方向通信が注目される流れがあったが、それは徐々に落ち着きつつあるようだ。

その上で、次の課題としてHTTP通信そのものを効率化する流れが起きつつある。利用者の増加や既存のサービスでの通信量の増加は言うまでもなく、双方向通信などによるリアルタイム性の向上、スマートフォンなどのモバイルデバイスの急速な普及などによって、HTTP通信に関する技術は急速に多重化や圧縮などの効率化を重視する流れに向かいつつある。

ウェブにおける双方向通信技術

近年のウェブサービスでは、リアルタイムかつダイナミックにコンテンツを書き換えるために、Ajaxなどを用いてサーバーとブラウザーの間で非同期通信を行う手法が見受けられる。しかし、それらの手法は旧来から存在していた技術を利用して実現しているため、ネットワークにかかる負荷の大きさや消費するリソースの多さ、開発のしにくさなど複数の問題を抱えており、それらを解決する代替手段が求められていた。

サーバーとブラウザー間の双方向通信 WebSocket

このような状況の中、ウェブ系技術者の注目を集めている技術の1つに、WebSocketがある。WebSocketは、サーバーとブラウザーの間で双方向のリアルタイム通信を可能にすることを目的として開発された技術である。HTTPのUpgradeヘッダーフィールドを用いて確立済みのTCPセッションを再利用することでそれを実現する。JavaScriptのAPI部分をW3CのWeb Applicationsワーキンググループが、プロトコル部分をIETFのHYBIワーキンググループがそれぞれ担当して標準化が進められた。2010年に一度、仕様上のセキュリティー問題が発見された影響で遅れが出たものの、2011年12月にはプロトコル部分がRFC 6455 The WebSocket Protocolとして標準化された。

これによりいったんの標準化が終了したWebSocketプロトコルだが、2012年2月には新たにフレームごとの圧縮や通信の多重化、タイムアウト時の仕様などを追加することが決定され、現時点ではそれらの仕様策定や議論が引き続き進められている。

2012年5月現在、RFC 6455に対応したMozilla Firefox 11およびGoogle Chrome 16といったブラウザーがリリースされており、Internet ExplorerやSafariにおいても開発版で実装が完了している。また、すでにこの技術を利用したウェブアプリケーションもリリースされつつあり、今後のさらなる普及が期待される。

クライアント間の双方向通信 WebRTC（RTCWeb）

ウェブで双方向通信を実現する技術としてもう1つ、注目を受けつつあるものにWebRTC(*1)が挙げられる。WebRTCはWebSocketと異なり、クライアント同士のP2P通信を実現する技術である。主にオーディオやビデオに主眼を置いたものであり、ブラウザー上で通話やビ

デオチャットのようなアプリケーションを実現することを可能とする。一般的に、IPv4インターネットにおいてクライアント同士で直接通信を行うことはNATによって制限されるが、WebRTCではSTUN(*2)やUDPホールパンチング(*3)などの技術を用いて問題をクリアしている。これも、API部分をW3CのWebRTCワーキンググループが、プロトコル部分をIETFのRTCWebワーキンググループがそれぞれ標準化に向けて活動中である。扱うデータが主にオーディオやビデオであるため利用するコーデックの取り決めも併せて行われているが、特許などの権利問題や各ブラウザーベンダーの意向の相違などにより、現時点で標準コーデックの決定には至っていない点など、まだ策定中という面が大きい。2012年5月時点でGoogle ChromeとOperaの開発版に試験実装が完了しており、Mozilla Firefoxは公開されていないものの、2012年3月にパリで開催されたIETF 83の会場においてMozillaの提唱するID認証システムであるMozilla Personaと組み合わせたデモを行った。

HTTP/2.0 策定に向けての方針と提案

2012年初頭、IETF HTTPbisワーキンググループは、これまで行ってきたHTTP/1.1に対する修正の標準化が完了に近づいていることから、HTTP/2.0の仕様策定および標準化を次の目標として定めることを発表した。

HTTP/2.0を策定するにあたって、目標として現行のHTTP/1.1よりもネットワーク資源を有効活用すること、HTTP/1.1からセマンティクスを変更せずに容易に相互変換が可能で互換性が確保できることなどが挙げられた。草案の募集は、インターネット・ドラフト形式で2012年6月15日までに提出となっている。同時にBasic認証、Digest認証に代わる新しい認証手段の策定も行うとしており新しい認証手段の草案も募集している。

IETF 83ではHTTP/2.0への提案として、次の4つが発表された。

・Mike Belshe氏ら（グーグル）のSPDY
・Gabriel Montenegro氏ら（マイクロソフト）のHTTP Speed and Mobility
・Willy Tarreau氏（HAProxy Project）やAmos Jeffries氏（Squid Project）らのNetwork-Friendly HTTP Upgrade（Intermediary Requirements）
・Roy Fielding氏（Apache Foundation, アドビシステムズ）のWaka

SPDY

SPDY（SPeeDY）は、ウェブにおける通信の多重化、優先度設定、圧縮およびサーバーからのプッシュを提供するプロトコルで、2009年ごろから開発が進められ、現時点でGoogle Chrome 9以降およびMozilla Firefox11以降に実装されている。GoogleやTwitterなどのウェブサービスですでに利用されていることから現時点でデプロイは完了しているとしているが、いずれも大規模サイトであり、中小規模のウェブサイトにおける導入の難易度や効果などは不明だといえる。また、SPDYはプロトコルとしてTLS（Transport Layer Security）(*4)による暗号化がほぼ必須といっていいため、コンテンツ事業者に対する負荷が増大すると考えられるが、提案者はRC4（Rivest's Cipher 4）を用いた暗号化やハンドシェイクに必要なCPUリソースは低く、証明書も無料で取得でき、実際にTLSを使用するSPDYのほうが従来のHTTPよりも高速であるという調査結果を提示している。しかし、TLSが必須になると、今までリバースプロキシ(*5)やロードバランサー(*6)、SSLアクセラレーター(*7)などを用いてバックエンドに平文通信を利用していたコンテンツ事業者については、規模の大小はさておき、設備の増強を余儀なくされることは容易に想像できる。また、今回の提案の中で唯一、HTTP/1.1から通信を開始することができない点が気になるところである。

HTTP Speed and Mobility（S+M）

HTTP Speed and Mobilityは、前述した双方向通信技術であるWebSocketでセッションを確立し、その中でSPDYの提案を利用する提案である。この提案では、そもそも暗号化が要求されない、または不可能な通信も多く存在する中、現状のHTTPを置き換えるプロトコルであるHTTP/2.0において暗号化を必須にしてはならないという主張のもと、TLSによる通信をオプションとしている。そのためTLSを前提とするSPDYと異なり、最初はTLSではないHTTPから通信を開始することができ、既存のHTTP実装や現状のユーザーの利用法との親和性が高いと考えられる。

Network-Friendly HTTP Upgrade

Network-Friendly HTTP Upgradeは、プロキシやロードバランサーなどクライアントとサーバーの間でHTTPを処理する機器やソフトウェアが現状持っている課題やプロトコルに対する要求などをまとめ、各要素の長さの埋め込み、頻繁に用いられるヘッダー名やメソッド名の短縮、バイナリエンコードの利用などによるパースにかかる資源の削減や、ユーザーエージェント文字列(*8)やホスト名などの通信セッション内で共通な情報やリファラやクッキーなどの連続したリクエストで共通な情報、メッセージを分類して共通な情報は再送しないことによる通信量の削減、アウトオブオーダー処理(*9)や多重化による資源の有効利用などを提案するものである。

Waka

Wakaは、現状のHTTPが抱える多くの問題点を根本的に解決することを目的とした提案である。現在のHTTP通信における冗長なシンタックス(*10)の改善や通信のコントロール情報からキャッシュコントロール情報まで、対応する通信レイヤーが大きく異なるデータが混在している問題の改善、新規メソッドの導入、パイプライニング(*11)、多重化などによって新プロトコルを制定し、HTTPを置き換えるものである。本提案の起源は古く、2002年ごろからApacheConなどで何度か発表されており、一定の評価は受けている。しかし、セマンティクスも大幅に改変してしまうことから、HTTP/2.0として採択される見込みは薄いのではないかと考えられており、あまり取り上げられてはいないようである。この提案に関しては2012年5月現在、正式な草案としては提出されていない。

以上の4つが、2012年5月の時点で確認できるHTTP/2.0への提案である。Wakaを除くすべてが現時点で正式に草案として提出されており、今後はメーリングリストを中心に議論が行われることになる。

個人的な見解としては、決定的な単一の提案というものはないと思っており、今後取捨選択を行うことや、そもそもの前提に関して議論を深めるなどが行われた上で、実際のHTTP/2.0の対象として策定されていくのではないかと思われる。

HTTP/2.0における新しい認証手段の策定については、2012年5月の時点で正式に提出されている草案はなく、IETF 83の会場においても発表は見受けられなかった。ただし、HTTPの新しい認証に関しては、HTTP/2.0の標準化が始まる以前からhttp-authという公式のメーリングリスト（ただしWGではない）があり、そこでいくつかの提案が行われている。その中の1つに日本の産業技術総合研究所が開発しているHTTP向けの新しい認証手段である「HTTPパスワード相互認証プロトコル」(*12)があり、標準化を目指しHTTP/2.0の提案として正式に提出される見込みである。

加速するウェブブラウザーの革新とプロトコルの変化

ウェブブラウザーの普及だけでなく、すべての通信がHTTPの上で行われるような動きはとどまるところを知らない勢いになっている。

今後も、プラットフォームとしてのウェブブラウザーの革新や、その上で行われるプロトコルの変化は当面続くと思われ、その流れはより大きく加速していくように思われる。

（*1）RTCWeb：IETFではRTCWeb、W3CではWebRTCという略称でそれぞれ呼ばれている。
（*2）STUN（Simple Traversal of User Datagram Protocol through Network Address Translators）：UDPで双方向リアルタイム通信を行う際に、NATによる制限を回避するための標準化されたプロトコル。
（*3）UDPホールパンチング：NAT通過のための技術。
（*4）TLS（Transport Layer Security）：SSL（Secure Socket Layer）をもとにIETFが標準化したセキュリティー機能の規格。公開鍵暗号基盤（Public Key Infrastructure、PKI）を用いて接続相手を確認し、通信を暗号化する。
（*5）リバースプロキシ：キャッシュなどを目的としてウェブサーバーサイドに設置される、特定のサーバーに対する通信を代理で行うサーバー。
（*6）ロードバランサー：負荷分散装置。
（*7）SSLアクセラレーター：SSLによる暗号通信で送受信されるデータの暗号化・復号を高速に行う専用装置。
（*8）ユーザーエージェント文字列：サーバーに対して申告される、ユーザーエージェントの識別名。ユーザーエージェント（User agent、UA）とは、特定のプロトコルに基づいて通信を行い、利用者に結果を表示する機能を持ったソフトウェア。ウェブブラウザーはウェブ閲覧のためのユーザーエージェントの一例。
（*9）アウトオブオーダー処理：依存関係にない複数の処理を、本来の順番に関係なく効率が良くなる順序で実行する処理方式。
（*10）シンタックス：プログラムやプロトコル上の構文。
（*11）パイプライニング：コンピュータの高速化技術の1つ。処理要素を直列に連結し、ある要素の出力が次の要素の入力となるように配置して平行処理する技術。HTTPにおいては複数のリクエストを一度に送信しつつ、同時並行でレスポンスを受信することをいう。
（*12）HTTPパスワード相互認証プロトコル：産業技術総合研究所とヤフーとの共同研究の成果によるもので、当社レピダムも開発に携わっている。

［インターネット白書ARCHIVES］ご利用上の注意

このファイルは、株式会社インプレスR&Dが1996年～2012年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書ARCHIVES」として以下のウェブサイトで公開しているものです。

http://IWParchives.jp/

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、データ、URL、名称など）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真・図の作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したりすることはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用される際は、出典として媒体名および年号、該当ページ番号、発行元（株式会社インプレスR&D）などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&D（初期は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

お問い合わせ先 | 株式会社インプレスR&D | ✉ iwp-info@impress.co.jp