HTTP-related WG Report (IETF87)

株式会社レピダム 林 達也
HAYASHI, Tatsuya
lepidum Co. Ltd.
IETF87報告会 2013/9/5

Agenda

- 自己紹介
- 参加の背景・経緯
- OpenID Meeting@ IETF
- httpbis
  - interim meeting
- httpauth
- oauth
- scim
- その他
  - rtcweb, websec, json

IETF 87

- Berlin, Germany
- July 28 - August 2, 2013

自己紹介

- 名前
  - 林 達也
- 所属
  - 株式会社レピダム
    代表取締役
    - https://lepidum.co.jp/
  - OpenIDファウンデーション
    ジャパン プロデューサー
  - Identity Conference
    (#idcon)
  - Internet Society
    Japan Chapter
    プログラム委員(2013)

- 業務領域
  - 標準化支援
  - 認証・認可, アイデンティティ、プライバシー
  - ソフトウェアセキュリティ, 脆弱性
  - ネットワーク技術
  - 言語処理系

経緯・背景

- 「HTTP相互認証プロトコル」の標準化支援
  - httpauth WG(Sec Area)
    - https://tools.ietf.org/html/draft-oiwa-http-mutualauth
  - (独)産業技術総合研究所様の研究成果
    - https://www.rcis.aist.go.jp/special/MutualAuth/
- IETFや標準化との関わり
  - IETF76広島から
  - 主にHTTP/Webと認証を中心に
- いくつかの企業様向けに、標準化支援や最新動向のコンサルテーション等

Applications Area概要

- 主にアプリケーション層に属する事象を扱う
- 15のアクティブなWG
  - appsawg　Applications Area Working Group
  - core　Constrained RESTful Environments
  - httpbis　Hypertext Transfer Protocol Bis
  - (hybi　BiDirectional or Server-Initiated HTTP)
  - (jcardcal　JSON data formats for vCard and iCalendar)
  - json　JavaScript Object Notation (NEW)
  - paws　Protocol to Access WS database
  - precis　Preparation and Comparison of Internationalized Strings
  - (qresync　IMAP QRESYNC Extension) (NEW)
  - (repute　Reputation Services)
  - scim　System for Cross-domain Identity Management
  - (spfbis　SPF Update)
  - urnbis　Uniform Resource Names, Revised
  - websec　Web Security
  - weirds　Web Extensible Internet Registration Data Service
- BoF
  - dmarc　Domain-based Message Authentication, Reporting & Conformance

TBD※括弧書きは今回Meetingが開催されていないWG

Online/Digital Identity & Privacy

- Online/Digital Identity & Privacyへ重要度と注目度の高まり
  - しかし、日本は**まだ**あまり…
- ISOCでもPrivacy & Identityは重要な課題
  - 技術的には認証・認可・セキュリティといった分野から
  - 技術だけでは解決できない
- IETF/W3C等でも横断的に扱われている
  - OAuth(OAuth2.0)
  - OpenID(OpenID Connect)
  - Federated Social Web

OpenID Meeting at IETF87

- IETF開催初日の日曜日に同会場で併催
  - Interoperability
  - Compliance
  - Using the OAuth Assertion profile
  - Bootstraping a Web session from a native client
  - Non-Web clients
  - RS-AS communication
  - OpenID 2.0 to Connect transition

- OpenID Foundationはもちろん、ISOC、IETFを始めとした組織から、アイデンティティ、認証・認可の専門家が集まって関連する仕様について議論しているので、興味がある方は日曜日の昼間から参加しましょう :-)

OpenID after IETF87

- Second OpenID Connect Implementer's Drafts Approved!
  - memberの投票により可決

Hypertext Transport Protocol Authentication WG

- 現在の機能の不足や安全性等、課題の多いHTTPプロトコルの認証機構を、新しく安全にすることを目指す
  - TLSを用いる方法やHTMLのフォーム認証はスコープ外
- 新しい認証をExperimental RFCとして策定
  - 現在ある複数の提案を統合したり選んだりするのではなく相互にレビューする形
  - 仕様と実装とどっちが先かの問題を避ける
- BasicおよびDigestの国際化、Digestのアルゴリズム更新もスコープ
  - こちらはStandard Track RFCを目指す

httpauth WG in IETF87

- Basic認証の国際化
  - WWW-Authenticateにcharset属性追加
  - UTF-8に統一
  - precis WGへHTTPAuthPrepのdraftを提出(産総研大岩先生、慶應大学根本さん)
    - https://tools.ietf.org/html/draft-oiwa-precis-httpauthprep
- Digest認証
  - アルゴリズムにSHA2-256, SHA2-512/256を追加
  - Multiple Auth対応
  - 国際化はBasicと同様
- Evalution Criteria for Experimental Draft
  - Security Considerationの明記
  - 実装における規制(自由度の確保と暗黙の禁止)
  - 既存インフラとの整合性の担保(相互運用性)
  - パフォーマンス上の制約を課さない
- WG Itemsの確定
  - Mutual Auth & Auth Extension
  - HOBA
  - SCRAM

Web Authorization Protocol WG

- RESTで用いる認可のフレームワークOAuth
  - OAuth 2.0のコア部分はすでにRFC発行済 (RFC6749, 6750)
- 現在はトークンのフォーマットや周辺エンドポイント等の議論中
- Recharteringの議論も

oauth in IETF 87

- Dynamic Client Registration
  - 継続して議論中
  - 新たにSCIM baseの提案も
- JWT&Assertion
  - 8/8にWGLCを迎える(た)
- OAuth 2.0 Message Authentication Code (MAC) Tokens
  - https://tools.ietf.org/html/draft-ietf-oauth-v2-http-mac-04
- OAuth 2.0: Audience Information
  - https://tools.ietf.org/html/draft-tschofenig-oauth-audience-00
- proof-of-possession
  - 昔Holder of Key(HoK)と呼ばれていた提案
- Token introspection
  - http://tools.ietf.org/html/draft-richer-oauth-introspection-04
- Security issue: multiple apps can register for the same URI scheme
  - https://tools.ietf.org/html/draft-sakimura-oauth-tcse
- JSON Metadata for OAuth Responses
  - https://tools.ietf.org/html/draft-sakimura-oauth-meta
- CoRE authorization

Info: OAuth2.0, OIDC & UMA Interoperability

- The 2013 OAuth2.0, OIDC and UMA Interop event is co-sponsored by the MIT-KIT, the Internet Society (ISOC) and the Kantara Initiative.
  - Dates: Thursday & Friday October 31st and November 1st, 2013.
    - (This is the Thursday & Friday prior to IETF88 in Vancouver, BC.)
  - Venue: Building W92, MIT Campus, Cambridge, MA, USA.
  - The organizers are Roland Hedberg and Thomas Hardjono.
  - https://kit.mit.edu/events/oauth20-oidc-uma-interoperability

AuthNとAuthZ

- Authe**N**tication(認証)とAuthori**Z**ation(認可)は別のものです！(主体に注意)
  - 混乱の原因例
    - OAuth2.0はOAuth**Z**です！(認可)
    - httpauth WGの扱うものはAuth**N**です

System for Cross-Domain Identity Management WG

- アイデンティティに関するプロビジョニング関連の標準化仕様のWG
  - スキーマ定義
  - ユーザの作成、修正、削除の操作セット
  - スキーマディスカバリ
  - 検索と読み取り
  - バルク操作
  - LDAPオブジェクトクラス(RFC2798)のinetOrgPersonとスキーマとのマッピング
- HTTP上のRESTfulなAPI
  - CRUDでの操作
- 昔は"Simple Cloud Identity Management"だった

scim in IETF87

- Core Documentは-02が出る(出た)
  - 基本はIssueを解決し続けてWGLCを目指す流れ
- Use CaseのDocumentの議論
  - ユーザシナリオやユースケース、Requirements
- OAuth2 SCIM JIT Client Registrationの提案
  - 色々Conflictしていそう…
- Interop at IETF88 Vancouverの提案
- WG Conference Calls
  - 隔週水曜日(11 AM PST / 7 PM UTC)
- 最終段階が近いため大きな話題はあまりない
  - 参加者も非常に厳選されていた
  - …と前回も書いていたのですが…

Hypertext Transfer Protocol Bis WG

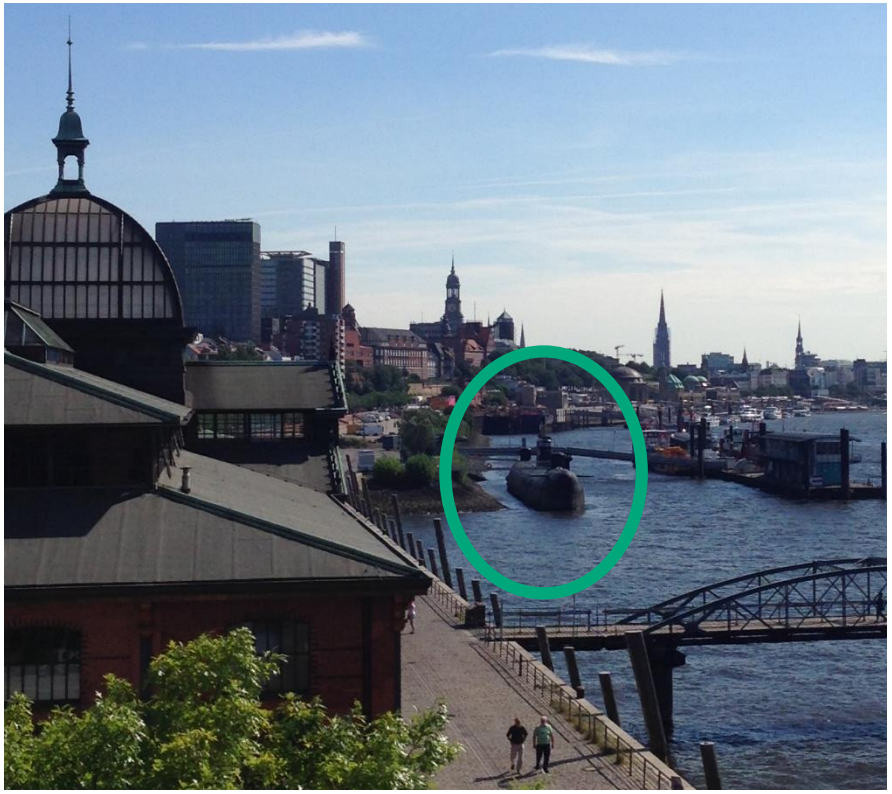
- HTTPのプロトコルを扱っているWG
  - 現在、HTTP/2.0を仕様策定中
  - 以前はHTTP/1.1の曖昧さを廃し、適切に仕様定義しなおすことを目指していた(1.1 はWGLC中！->まだ…)
- HTTP/2.0の目的
  - 環境を限定しないパフォーマンス改善
  - ネットワーク資源の効率的な使用
  - 現代的なセキュリティ要件および慣習の反映
- 仕様概要
  - スタートポイントはGoogleのSPDYプロトコル

httpbis in IETF87

- HTTP 1.1bis status
- Header Compression Benchmark
  - https://tools.ietf.org/agenda/87/slides/slides-87-httpbis-0.pdf
- HTTP and Encryption (Liaison with TLS WG and W3C)
  - "HTTP/1.1 has no Mandatory to **Implement** Security"
  - "SPDY introduced Mandatory to **Use** Security"
- HTTP2.0 with a TSV Eye

about httpbis Interim Meeting #3

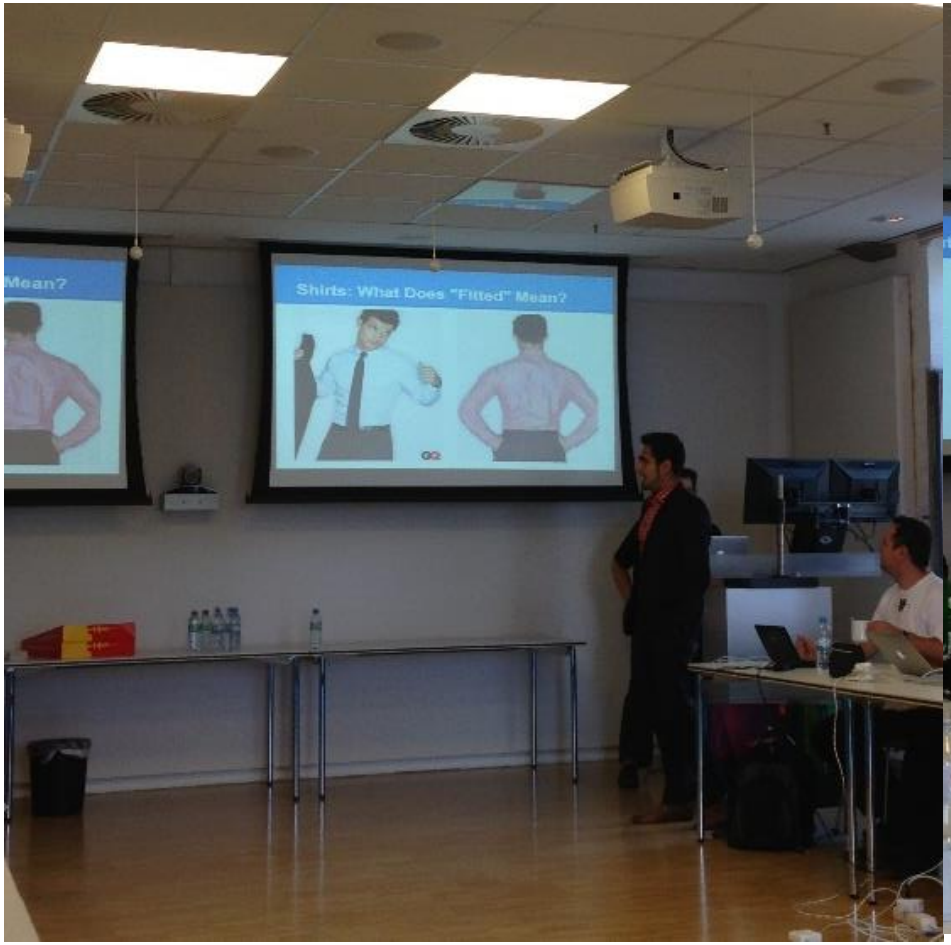
- 2013/8/5～8/7
  - IETF 87後にHamburgへ
- Adobe German Office はすばらしかったです
  - 会議室の窓から潜水艦(本物)が見えるオフィスとかそうそうない
  - 心地良い日差しと気持ち良い風が入ってくる中、優雅にプロトコル談義(英語)

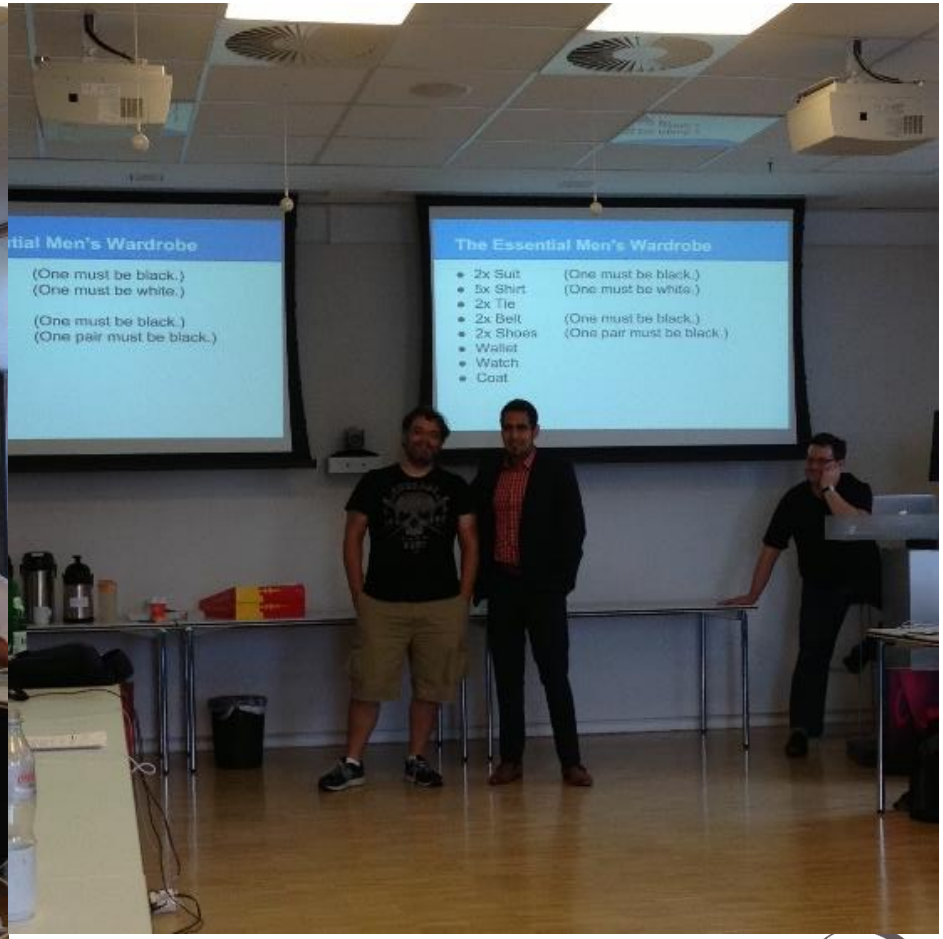


httpbis Interim Meeting #3

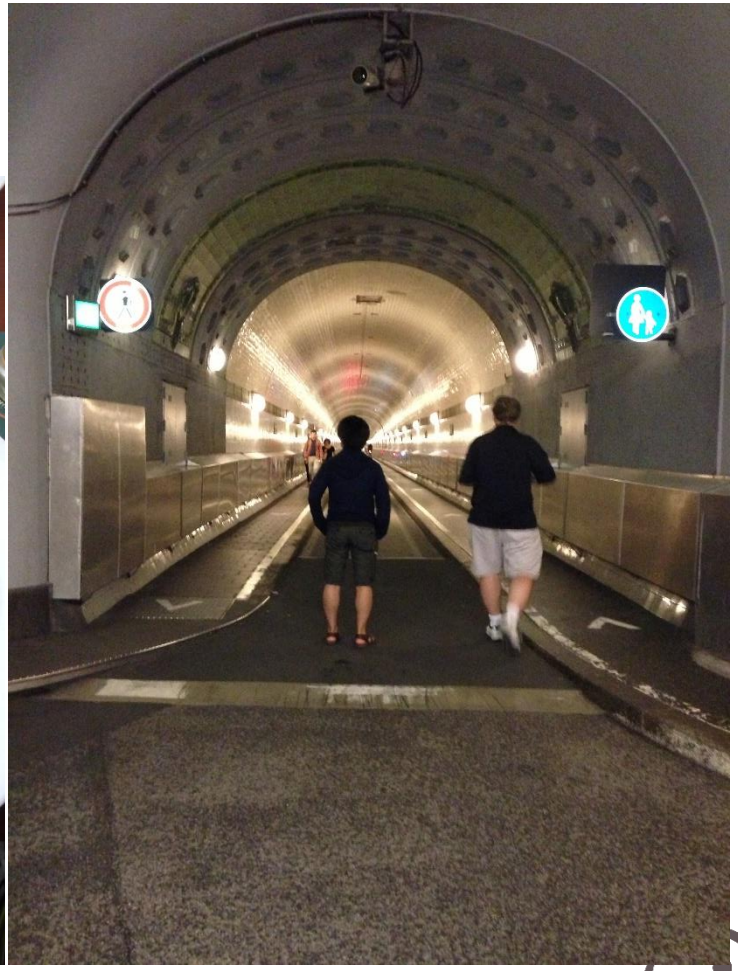
- 実装者からのfeedback & Issue整理
  - HTTP/2.0ではRC4禁止
    - "RC4 - prose recommendation that RC4 ought not be used. "
    - https://github.com/http2/http2-spec/issues/172
  - ALPN vs NPN再び
    - クライアント側からコントロールしたい(のでNPNがよかった)
    - SPDYを考えたら実際にはNPNとALPNの両方サポートしないといけない
  - Continue Flag -> Continue Frame
  - ServerPush(PUSH_PROMISE)
  - Header-Compression -> HPAC
  - QA and Test
- 実際にはどんな感じだったか？
  - "Compression is not hard to implement.
    Implemented in 2 days (both sides), 400 lines of C++." (minutesより)
- Interop! (世界初のHTTP/2.0相互接続試験)
  - 実は日本からの実装が超絶優秀
    - nghttp2 (Tsujikawa-San) [C/C++] / iij-http2 (Ohtsu-San) [node.js]

Interim Meeting #3 Photos





Interim Meeting #3
Social Event Photos



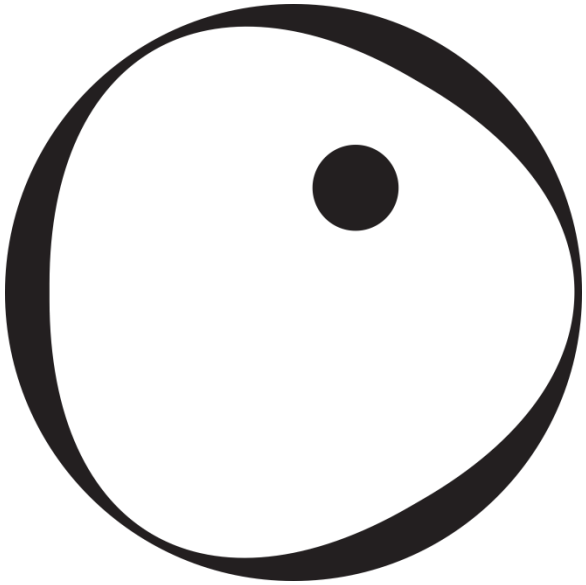
etc WG in IETF87

- websec
  - Public Key Pinning Extension for HTTP(HPKP)がWGLCへ
  - Session Continuation problem statement
    - Bearer Taken, Cookie Scope, Cookie Availability, logout, Cookie behavior
- rtcweb
  - SDES, MMUSIC Unified Plan, Security, UseCase, Data Channel
- json
  - rfc4627bis
- jose
  - JWx仕様の策定まであと一歩といったところ
- 未開催
  - jcardcal, hybi(websocket)

まとめ

- Web関係の話題が衰えずに増えている
  - 他のArea との温度差が激しい感触
- ユースケースとしてモバイルが重要に
  - もうクライアントはPCではない
- 認証・認可・プライバシー
  - 従来のセキュリティとは若干違う領域を扱いつつある
    - 特にプライバシー
  - InternetとWebが普及し、強力な力を持つようになる/なった世界で個人の権利をどう捉えるのか

Any Questions? / Please Feedback!



lepidum

https://lepidum.co.jp/