IETF86 HTTP-related WG Report

株式会社レピダム 林 達也
HAYASHI, Tatsuya
lepidum Co. Ltd.
2013/4/18

lepidum
https://lepidum.co.jp/

Agenda

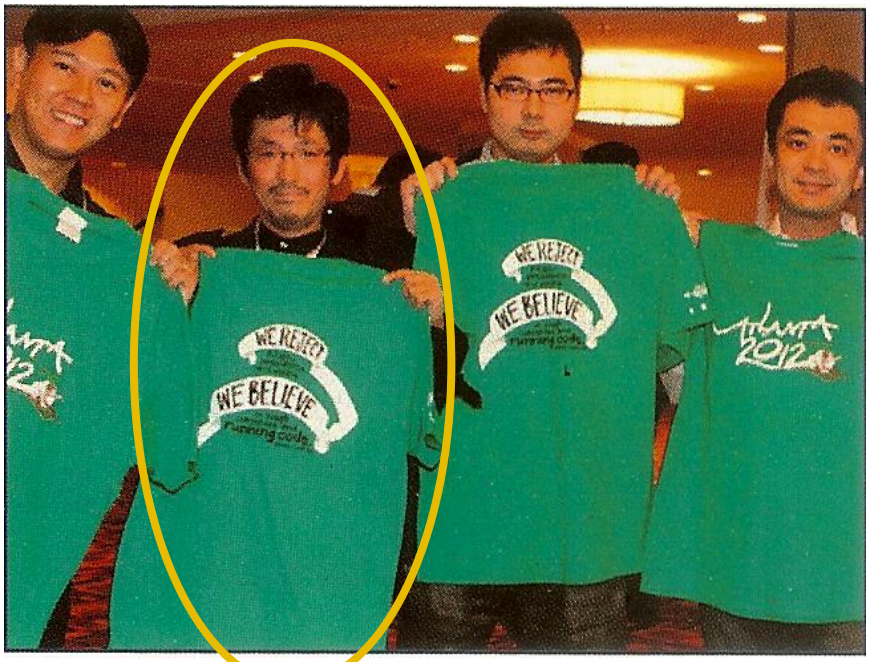
- 自己紹介
- httpbis
- httpauth
- oauth
- scim
- その他
  - rtcweb, websec, jose, j cardcal
  - json BoF, aggsrv BoF
  - OpenID Meeting

IETF 86

- Orlando, FL, USA
- March 10 - 15, 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 Producer
- 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
  - セキュリティ, 脆弱性
  - ソフトウェア, プログラミング言語, コンパイラ
- 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



from The IETF Journal
Volume 8, Issue 3 March 2013

Applications Area概要

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

※括弧書きは今回Meetingが開催されていないWG

Hypertext Transfer Protocol Bis WG

- いまAPPで一番HotなWG！
  - 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！)
- 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が仕様策定したSPDYプロトコル
  - しかし、既に仕様は分岐し始めている

httpbis in IETF86

- フレームの詳細な構造等の議論
  - ストリーム識別子を毎回含めるか
  - エラーに関する議論
  - その他
- CRIME Attackを踏まえたヘッダ圧縮の議論
  - デルタエンコーディングを用いる
- 基本的に合意形成を主眼にIssue Closeに終始
- 1月末のTokyoでのInterim Meetingのfeedbackも
  - その結果最初の実装向けdraftが近々出ることに

httpbis after IETF86

- ... in tls WG(IETF86)
  - HTTPS通信時のためのプロトコルネゴシエーション
  - 従来のNPNではなくALPNを用いることに
- 頻繁なInterim Meetings
  - 6月中旬はベイエリアで
  - 8月上旬はドイツで（！？）

HTTP/2.0詳細(宣伝)

- HTTP/2.0の最新情報や詳細については、弊社清水が発表などをさせて頂いております
  - Internet Watchコラム「HTTP 2.0の最新動向」
    - http://internet.watch.impress.co.jp/docs/column/http20/latest.html

Hypertext Transport Protocol Authentication WG

- いまSecでHotなWGのひとつ！
  - IETF BlogにもIETF Journal March 2013にも載っています
    - http://www.ietf.org/blog/2013/03/welcome-to-ietf-86/
    - http://www.internetsociety.org/articles/ietf-ornithology-recent-sightings-4
- 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

httpauth WG in IETF86

- BoF当日朝(!)に “WG Action: … (httpauth)”
- Experimental RFCを策定することが目標となる異例のWGとなった
  - 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かたちとなる
  - 仕様と実装とどっちが先かの問題を避けるため
- BasicおよびDigestの国際化、Digestのアルゴリズム更新もスコープに
  - こちらはStandard Track RFCを目指す

WGへの道

- IETF79: APP Areaでhttp-auth MLオープン(reboot)
- IETF80: Bar BoF開催
- IETF81: httpauth BoFが公式にAgendaに掲載されたが突然のCANCELED!!!
- IETF82: (ネゴシエーション…)
- IETF83: httpbis WGで新たなHTTP認証について提案が募集される
- IETF84: httpbis WGはHTTP/2.0に注力(APP)
  - 認証は議論は継続し、別途Experimental RFCをゴールとしたWGを立ち上げる方針に(SEC)
- IETF85: httpauth BoF#2が開催されWG化の検討を議論
  - しかし結論は出ず…

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(6749, 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

oauth in IETF 86

- Dynamic Client Registration
  - OpenID Connect の物と統合される方向に
- アサーション
  - SAMLのものとJWTのもの
- MAC Token等
  - やはりBearerでないトークンへの需要は大きい
  - 一度立ち消えたが議論継続中

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 IETF86

- Search Enhancement
- Clarify the Spec on Multi-Tenancy
  - Multi-Tenancyに関しては一応仕様外に(non-normative)
- SCIM Profile For Enhancing Just-In-Time Provisioningの提案
- SCIM SchemaのIssue整理
- 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
- 前回のtopicだったvCard Schemaとのマッピングは変更部分が大きいため採用しない方向に

etc WG

- rtcweb
  - コーデック戦争 (H.264 vs VP8) 終結か？
  - 名前混乱問題
    - RTCWEB? WebRTC?
    - "Name of the system" -> Confirmed that will be "WebRTC" from **now on**.
- websec
  - Session Continuation
    - Cookie認証を滅ぼす話がここでも提起される
- jose
  - JWx仕様の策定まであと一歩といったところ
- jcardcal (今回未開催)
  - vCard, iCalendar をJSONフォーマットにする

etc BoF

- json BoF
  - ひとまずECMAScriptとの非互換解消等の細かい修正を第一目標とすることとなった
  - 追加機能や周辺技術はそれが終わってから
- aggsrv (Aggregated Service Discovery) BoF
  - メールなども含めた様々なサービスの設定情報をaggregateして提供するメタデータの仕組み
    - .well-known / Defining Well-Known Uniform Resource Identifiers(rfc5785)

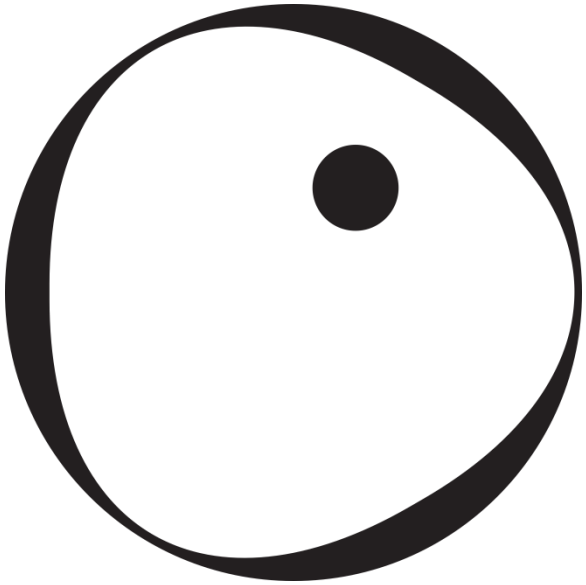
OpenID Meeting at IETF86

- 最近IETF開催初日初日の日曜日に同会場で併催
  - Implementer's Drafts
  - OAuth Security Discussion
  - Interoperability Discussion
  - Compliance Testing
  - Using OpenID Connect for unmodified non-Web clients / RS-AS Communication
    - PEOFIAMP Project(NRI/NII/東大/京大)
    - draft-sakimura-oidc-structured-token
    - draft-sakimura-oidc-extension-nonweb
  - 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 :-)

まとめ

- Web関連の話はどんどん増えています
  - 今回はHTTP関連のWGを中心にしましたが、Application Areaは他にも色々あって正直カバーしきれていません
  - もっと参加者や専門家が増えて欲しい
  - 皆様も是非！
- JSONの潮流
  - 以前から用いられていたが、ついにjson WGができたり既存フォーマットをJSONにしたりと流れが加速している
- Webと認証・認可の領域は
  - 多くの人にユーザと関わる認証・認可、PrivacyやIdentityへの理解をもっと深め、広げていきたい

Any Questions? / Please Feedback!



lepidum