IETF85 Applications Area Report

株式会社レピダム 林 達也
HAYASHI, Tatsuya
lepidum Co Ltd.
2012/12/21

lepidum
https://lepidum.co.jp/

Agenda

- 自己紹介
  - 参加背景・経緯
- appsawg
- httpbis WG
- httpauth BoF
- scim WG
- Topic:
  - Privacy & Identity
- まとめ

IETF 85

- Atlanta, GA, USA
- November 4 - 9, 2012

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/
- 業務領域
  - セキュリティ, 脆弱性
  - 認証・認可, アイデンティティ、プライバシー
  - 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
  - IETF以外には、IIW, W3C等に参加

参加の背景・経緯

- IETF参加のきっかけは、「HTTP相互認証プロトコル」の標準化支援
  - (独)産業技術総合研究所様とヤフー(株)様の共同研究
    - https://tools.ietf.org/html/draft-oiwa-http-mutualauth
    - https://www.rcis.aist.go.jp/special/MutualAuth/
- 現在は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をさせて頂いております

HTTP and Web

- 『HTTPやWebはW3Cで標準化しているのでは？』
- 概ね以下の境界で担当範囲が分かれる認識
  - IETF ＝ プロトコル層以下
  - W3C ＝ API層以上

- hybi(WebSocket),rtcweb(WebRTC)が代表的

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
  - iri Internationalized Resource Identifiers
  - paws Protocol to Access WS database
  - precis Preparation and Comparison of Internationalized Strings
  - scim System for Cross-domain Identity Management
  - spfbis SPF Update
  - websec Web Security
  - weirds Web Extensible Internet Registration Data Service
  - eai Email Address Internationalization
  - (hybi BiDirectional or Server-Initiated HTTP)
  - (imapmove IMAP MOVE extension)
  - (repute Reputation Services)
  - (urnbis Uniform Resource Names, Revised)

※括弧書きは今回Meetingが開催されていないWG

Applications Area WG(appsawg)

- 特定のWG Itemではないが Applications Areaに属するものを扱うWG
- IETF84以降で作業完了した仕様
  - draft-ietf-appsawg-http-forwarded (RFC Editor Queue)
  - draft-ietf-appsawg-media-type-suffix-regs(RFC Editor Queue)
  - draft-ietf-appsawg-about-uri-scheme (RFC6694)
  - draft-ietf-appsawg-received-state (RFC6729)
- 進行中のdraft仕様
  - draft-ietf-appsawg-webfinger
  - draft-ietf-appsawg-json-{pointer,patch}
  - draft-ietf-appsawg-acct-uri
  - draft-ietf-appsawg-malformed-mail

appsawg in IETF85 (1)

- WebFinger
  - "WebFinger is a simple protocol used to discover information about people and entities on the Internet."
  - 誤解を恐れずにいえばfingerのWeb版
    - 但し個人的には意味合いはかなり異なってきていると感じる
- JSON関係
  - JSON Pointer/PatchがWGLC
  - JSON Content Rules
    - JSON Schemaの為の言語
    - JSON likeだがJSONではない
  - JSON WGの必要性
    - 賛成多数だったのでWG化されると思われる

appsawg in IETF85 (2)

- DMARC
  - "Domain-based Message Authentication, Reporting & Conformance"
    - http://www.dmarc.org/
  - standards trackかindependentかは不明だが、おそらくIETFで標準化の方向
- その他
  - apps-discuss MLの流量
  - URI関係
    - IPv6 Zone Identifiers in URIs
      - % or %25の話
    - acct-uri
      - acctURI = "acct:" userpart "@" domainpart

Hypertext Transfer Protocol Bis WG

- いまAPPで一番HotなWG！
  - 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
  - Rechaterの結果、HTTP/2.0という聞くだけで熱くなる仕様策定を開始
    - まだ始まったばかり
- 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
- スタートポイント
  - ベースはGoogleが仕様策定したSPDYプロトコル

httpbis in IETF85

- HTTP Upgrade Mechanism
  - SPDYではTLSのNPN(Next Protocol Negotiation)拡張を利用して、1.1からのUpgradeを実現している
  - HTTPSではないHTTP通信の際に、1.1からのUpgradeをどうするか？
  - いくつかの案
    - HTTP Upgrade ヘッダフィールド
    - DNS SRVレコード
    - HTTP/1.1レスポンスのヘッダ(HTTP/2.0サーバのport番号を含める)
- CRIME Attackを踏まえた圧縮に関する議論
- WebSocketを踏まえたFlow Controlの提案

httpbis after IETF85

- ... in tls WG(IETF85)
  - HTTPS通信時のためにhttpbisのChairがNPN拡張の標準化を提案
    - 「なぜTLSで？レイヤーバイオレーションでは？」「TCPレイヤでやるべきでは？」「TCPにはその為にポート番号がある」等
    - 継続議論に
- WGから-00 draftがpublishされた
  - https://tools.ietf.org/html/draft-ietf-httpbis-http2-00
- 2013/1/30 - 2/1にTokyoでInterim Meetingが開催されます
  - (が、もうほぼ〆切られてしまいました…)

HTTP/2.0詳細(宣伝)

- HTTP/2.0の最新情報や詳細については、当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
  - 「エンジニアサポートCROSS 2013」#cross2013
    - パネルへ登壇
    - http://www.cross-party.com/program/

HTTP Authentication Mechanisms BoF

- いまSecでHotなBoFのひとつ！
- 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

Official BoFへの道(1)

- IETF79
  - APP Areaでhttp-auth MLオープン(reboot)
- IETF80
  - Bar BoF開催
- IETF81
  - HTTP Authentication Mechanisms BOF
    - 突然のCANCELED!!!

Official BoFへの道(2)

- 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)

httpauth BoF in IETF85 (1)

- 5つの提案
  - HTTP Mutual Authentication / HTTP Auth Extention
    - draft-oiwa-http-mutualauth
    - draft-oiwa-http-auth-extension
  - draft-farrell-httpbis-hoba
  - montenegro-httpbis-multilegged-auth
  - draft-melnikov-httpbis-scram-auth
  - draft-williams-http-rest-auth

httpauth BoF in IETF85 (2)

- 約100人程の参加者で、Problem statementと5つの提案について活発な議論
- charter discussion
  - 「Experimentalの後、実際に利用されたものをStandardにすればいいのでは？」
  - WGで作業をすたいと思う人はどのくらいいるか？という質問に対して
    - 20～30人の挙手

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 IETF85

- vCardとのマッピングについて
  - vCardはいわゆる名刺のフォーマット
  - 最近ではアドレス帳等で使用されるケースが多い
- シリアライズのサポートフォーマット
  - JSON and/or XML
  - XMLを外すことについてのHumが行われXMLを今後サポートしないことに

Online/Digital Identity & Privacy (1)

- Web/HTTPと認証・認可に携わっている中で、Online/Digital Identity & Privacyへ重要度と注目度の高まりを最近強く感じる
- ISOCでもPrivacy & Identityは重要な課題
  - セキュリティとは独立した分野として扱われることが一般的になりつつある
- IETFでも、横断的に様々な場所で扱われている

- OAuth WG
  - 「認可」プロトコルの標準化
    - 元々はAPPのWGだったがSECへ移った
  - OAuth 2.0は2.5年程かかったがようやくRFC化
    - The OAuth 2.0 Authorization Framework
      - http://tools.ietf.org/html/rfc6749
    - The OAuth 2.0 Authorization Framework: Bearer Token Usage
      - http://tools.ietf.org/html/rfc6750
  - JSON Web Token (JWT)等のWG Itemが進行中
    - 次のItemを現在議論中

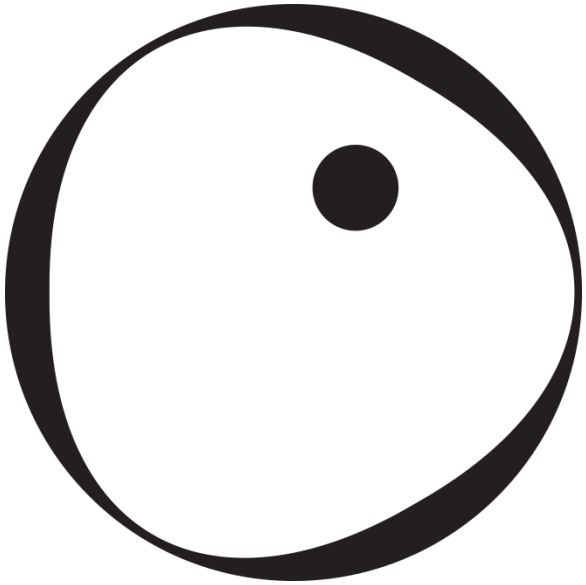
Online/Digital Identity & Privacy (2)

- Javascript Object Signing and Encryption(jose) WG
  - JSON Web Algorithms (JWA), JSON Web Encryption (JWE), JSON Web Key (JWK), JSON Web Signature (JWS)
  - OAuth 2.0等の様々な仕様で使われるフォーマットとして
- OpenID Meeting at IETF85
  - IETF開催初日に同会場で併催
  - OpenID Connect
    - OAuth 2.0をベースとした認証・認可のプロトコル仕様
  - BackPlane Protocol
  - Account Chooser

まとめ

- アプリケーションとひとことでいっても領域は広いので様々な層の人達と情報交換できれば
  - いまユーザが触っている領域はAppsAreaに！
  - 最近はWebと関わりのない領域の方が少ないと思うので、興味をもってもらえるとうれしい
  - 決して無駄にはならないと思います
- もっと参加者や専門家が増えて欲しい
- 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