

# HTTP-related WG Report (IETF89)

---

株式会社レピダム

前田 薫 (@mad\_p)

IETF89報告会 2014/04/11



# Agenda

---

- 自己紹介
  - 参加の背景・経緯
  - httpbis WG
    - designer meeting
  - httpauth WG
  - ace BoF
  - その他
    - json, oauth
- IETF89
    - London, UK
    - March 2-7



# 自己紹介

---

- 名前
  - 前田 薫
- 所属
  - 株式会社レピダム  
シニアプログラマ  
マネージャ
- コミュニティー活動
  - Lightweight Language
  - Identity Conference
  - http2勉強会
- 業務領域
  - 認証・認可、デジタル  
アイデンティティ、  
プライバシー
  - 標準化支援
  - ソフトウェアセキュリ  
ティ、脆弱性



# 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
  - New Attendee Badge →
  - HTTP/Webと認証を中心に
- 標準化支援や最新動向のコンサルテーション等を行っています



# httpbis WG

---

- Hypertext Transfer Protocol Bis
- HTTP/2最終段階に向けてラストスパート
  - 詳細すぎる仕様は切り離してhttp2を早く Last Callに持っていきたい
  - ヘッダ圧縮とセキュリティ
- HTTP/1.1 update
- Local Activity report (Jxck\_ + nunnun)



# HTTP/2

---

- HTTP/2.0 → HTTP/2
  - バージョニングしない
- 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
  - いくつかの提案の中からGoogleのSPDYプロトコルをスタートポイントに策定を開始



# HTTP/1.1とHTTP/2の違い

---

- HTTPヘッダーのバイナリ化
- HTTPヘッダーの効率化(圧縮)
- 多重化(Multiplexing)
- 優先制御(Prioritizing)
- 通信の開始方法
- TCPコネクションの利用方針
- etc...



# HTTP/2の議論 in IETF89

---

- HTTP/2はTLS必須? → 必須としない
  - HTTP/2 connection上でhttpスキームも送れる
- Last Callに向けて仕様の整備
  - あいまいな部分の明確化(SETTINGS、Same-Origin、gzip)
- Websocketサポート
- HTTP/2開始手順
  - ALPN、Alt-Svc(フレーム、ヘッダ)、DNS/SRV
- Priority Leveling
- HPACK脆弱性





# HPACK脆弱性

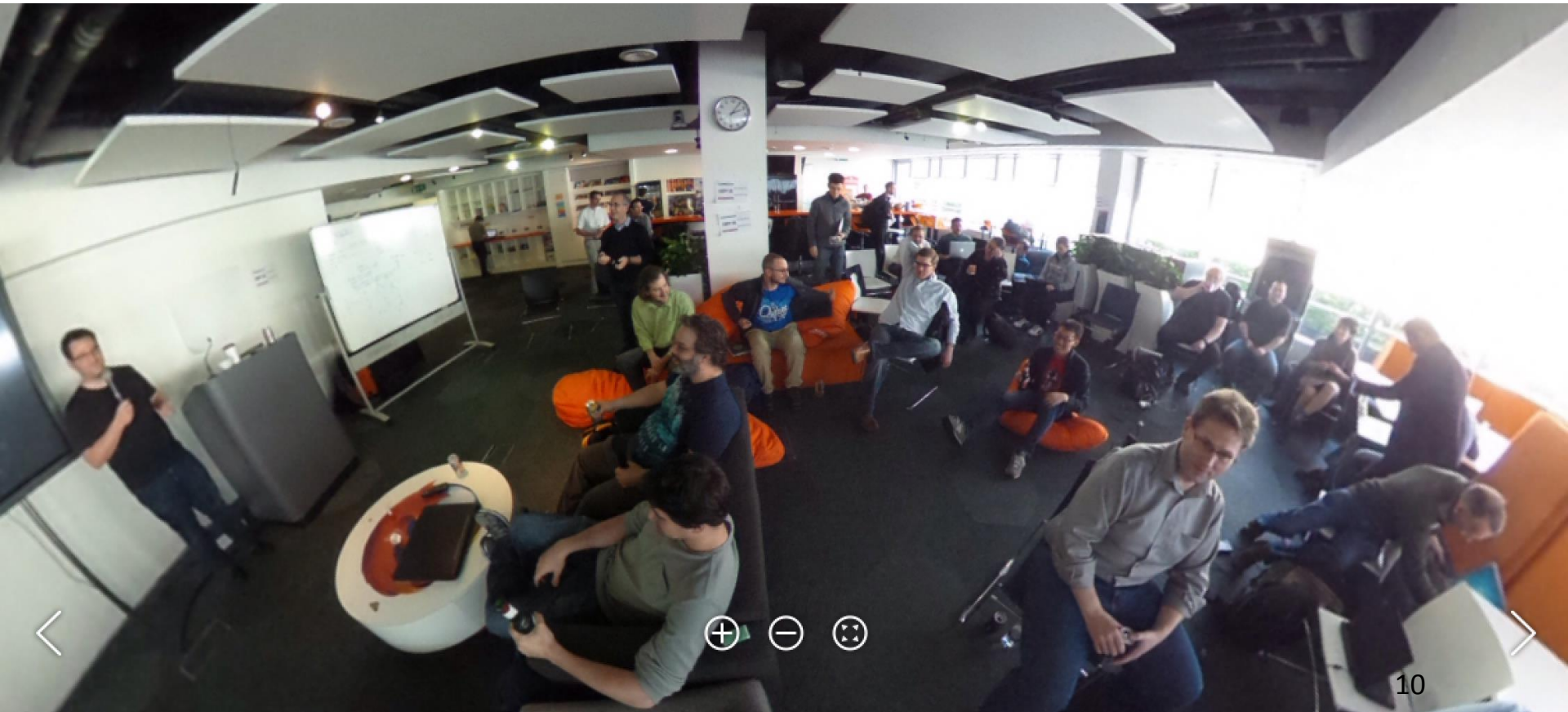
- Basic認証ヘッダをinjectしパケットサイズを観測
  - ヘッダ圧縮率がオラクルとして働く
  - 低エントロピーでなければあまりコワくない
  - クッキーはエントロピー高いがパスワードは?
- センシティブなヘッダは圧縮しない案
  - ホワइटリスト方式かブラックリスト方式を議論
  - 圧縮するなフラグを追加(個別設定)で合意、セキュリティ考察も追加
- 却下された案
  - MAX\_CONCURRENT\_STREAMを小さくすれば試行が少なくなるという案、一定回数の失敗で忘れる案、一定確率で圧縮しない案



# designer meeting 3/8

## ■ Mozilla London オフィスで開催

- [Preliminary Minutes](#)



# designer meeting トピック

- Padding
- HPACK
- SRV/DNS
- Alt-Svc
- Priority Leveling →
- Proxy
  - use-case, discovery



# Padding

---

- フレーム側の仕組みとしてPaddingを設ける
  - HPACK側はpaddingなし
- flow-controlにどう影響するの? など議論
- BREACH/CRIMEアタックに対しては、観測結果が確率的にしか得られないことで緩和
  - ドラフト10ではPaddingによる攻撃への効果は限定的であることも言及している



# httpbis今後の予定

---

- 4月 WG Last Call
  - 4/4 HTTP/2 draft 11、HPACK 07
  - IETF89、designer meetingの議論を反映
- 6月上旬、米東海岸で第6回interim
  - 6/5-6 New York
- 7月下旬、IETF 90 Toronto
- 8月 IETF Last Callをめざす



# httpauth WG

---

- Hypertext Transport Protocol Authentication
- 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 IETF89

---

## ■ Digest認証

- ユーザ名をハッシュ化する案 → サーバ側で照合できないので却下

## ■ Basic認証

- ユーザ名にコロンは含めないことを明示

## ■ ユーザ名、パスワードの国際化

- UTF-8 NFCに統一したいが、現状のブラウザ実装が必ずしも十分に対応していないこともわかった
- → precis WGで検討中。foldingでトルコ語が難しい



# ace BoF

---

- Authentication and Authorization for Constrained Environments BOF
- clientやresource serverが制限されている場合の認証・認可、channel bindingなどを考える
  - 制限されたリソースの例: ドアロック、血圧計
- ユースケース
- CoAP: Constrained Application Protocol
  - コンパクトなバイナリプロトコル (core WG)
  - HTTP/REST モデル, GET, PUT, DELETE, POST
  - DTLSによるセキュリティー





# Constrained nodes: orders of magnitude

## 10/100 vs. 50/250



- There is not just a single class of “constrained node”

- Class 0: too small to securely run on the Internet

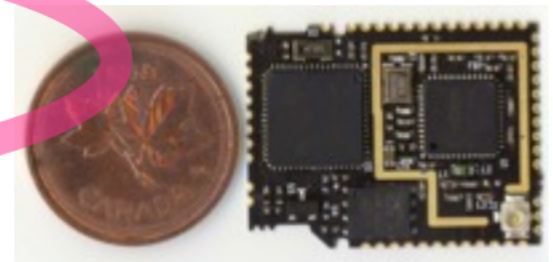
- “too constrained”

- Class 1: ~10 KiB data, ~100 KiB code

- “quite constrained”, “10/100”

- Class 2: ~50 KiB data, ~250 KiB code

- “not so constrained”, “50/250”



- These classes are not clear-cut, but may structure the discussion and help avoid talking at cross-purposes

Carsten Bormann

<http://www.ietf.org/proceedings/89/slides/slides-89-ace-2.pdf>

# Example: Container Monitoring



Ludwig Seitz

<http://www.ietf.org/proceedings/89/slides/slides-89-ace-3.pdf>

# ユースケース: コンテナモニタリング

---

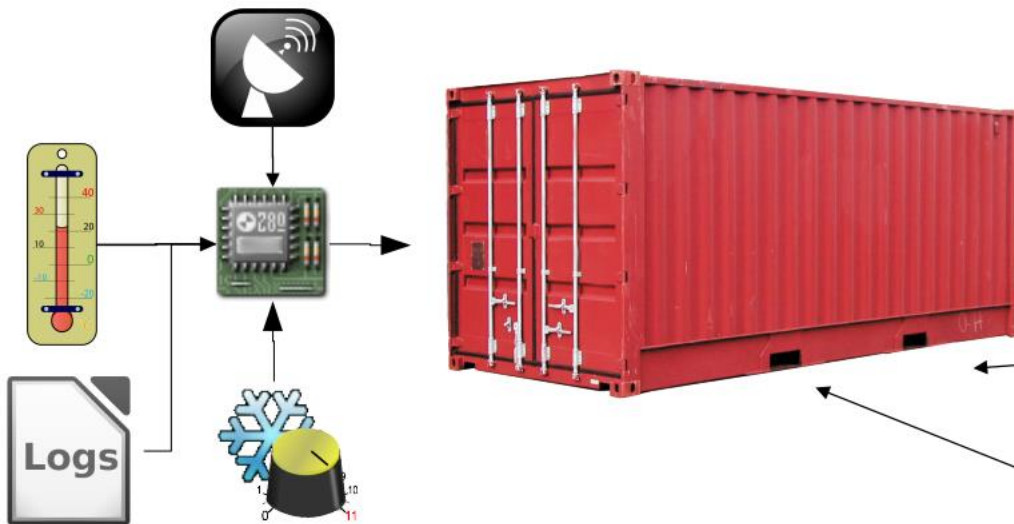
- 荷主がデバイスを入れる
- 海上ではオフラインになるがアクセス制限は必要
- 倉庫では庫内環境を見るためにアクセスが必要
- 運送時、トラックは×、電車は○などの制御のためにアクセスが必要



# Resources and Stakeholders


Resources:  
Sensors, Actuators, Data

Stakeholders



  
Owner

  
Storage

  
Transport

Different access  
modes (read/write)

Different access rights  
per stakeholder

Ludwig Seitz

<http://www.ietf.org/proceedings/89/slides/slides-89-ace-3.pdf>

# ace BoFの議論

---

- アーキテクチャスケッチとデザイン上の課題
  - multi-party security protocol
  - Session security
  - 鍵は Symmetric or Asymmetric?
- Gap Analysis
  - Kerberos, OAuth, PKI, AAAなどの既存モデルをaceに適用した場合のgapを検討
  - 例: Kerberosではアクセス制御ポリシーの記述言語がない、OAuthではCoAP/DTLS bindingがない、トークンが大きすぎる、など
- Charterの文書化
  - ブートストラップ問題をスコープに入れるか
  - appエリアなのかsecエリアなのか



# その他

---

- json WG
  - JSON RFCが更新されました! → RFC7159
- oauth WG
  - Dynamic Registrationの文書化
  - Security: client, AS, RS間の鍵配布問題など
- OpenID Connectミーティング
  - OpenID 2.0からのマイグレーション
  - Native App WG



# まとめ

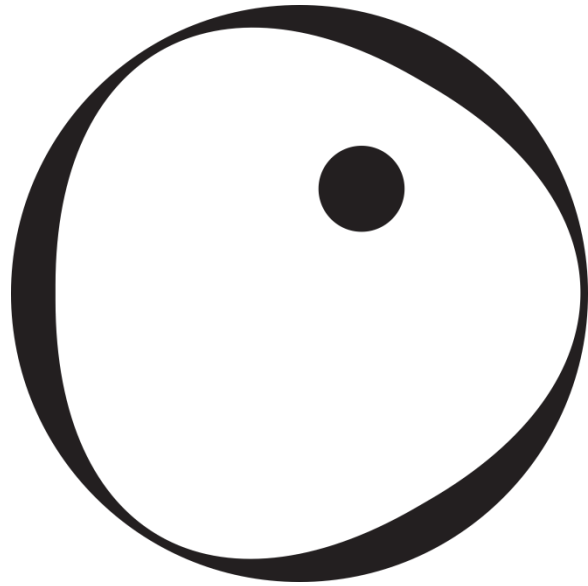
---

- HTTP/2 is coming!
  - SPDYベースのバイナリプロトコル
  - intermediariesでコネクションをたばねることも
  - ヘッダ圧縮とセキュリティーの問題を解決
- httpauthでは認証プロトコルにおける国際化も話題に
- ace BoFなどInternet of Things時代に向けての議論が始まっています



Any Questions? / Please Feedback!

---



**lepidum**

<https://lepidum.co.jp/>

mailto:maeda@lepidum.co.jp / twitter: @mad\_p

