IoT-related WG Report (IETF90)

株式会社レピダム

前田 薫 (@mad_p)

IETF90報告会 2014/08/25

Agenda

- 自己紹介
- 参加の背景・経緯
- core WG
- ace WG
- dice WG
- その他
  - json

- IETF90
  - Toronto, Canada
  - July 20-25

地下街

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ー、プライバシー
  - 標準化支援
  - ソフトウェアセキュリティー、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
  - IETF89から参加
  - 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しています

core WG (Wed Jul 23, Thu Jul 24)

- Constrained RESTful Environments
  - 制限された環境でのRESTfulアクセス
- CoAPプロトコル(RFC7252) 2014-06
  - http://coap.technology/
  - REST(request/response)モデル (cf. メッセージング)
  - 非同期通信(UDPベース)
  - ヘッダが小さい、パーズしやすい
  - HTTPとのマッピング
  - Discovery

core WGでの話題

- 実用化に向けた追加仕様の検討
- Blockwise Transfer
- Congestion Control
  - exponential back-offの工夫による性能向上
- HTTP-CoAP mapping proxy
- リンク表現のJSON版
  - RFC 6690の代わりにJSON

HTTP-CoAP mapping proxy

- HTTPクライアントがCoAPサーバーにリクエストするためのプロキシ
- media-typeマッピング
- コンテンツ表現形式変換
  - XML/EXI, JSON/CBOR
- リンク変換
  - ディスカバリ結果、リソースリンク
  - </sensors/temp>;rt="temperature-c";if="sensor"

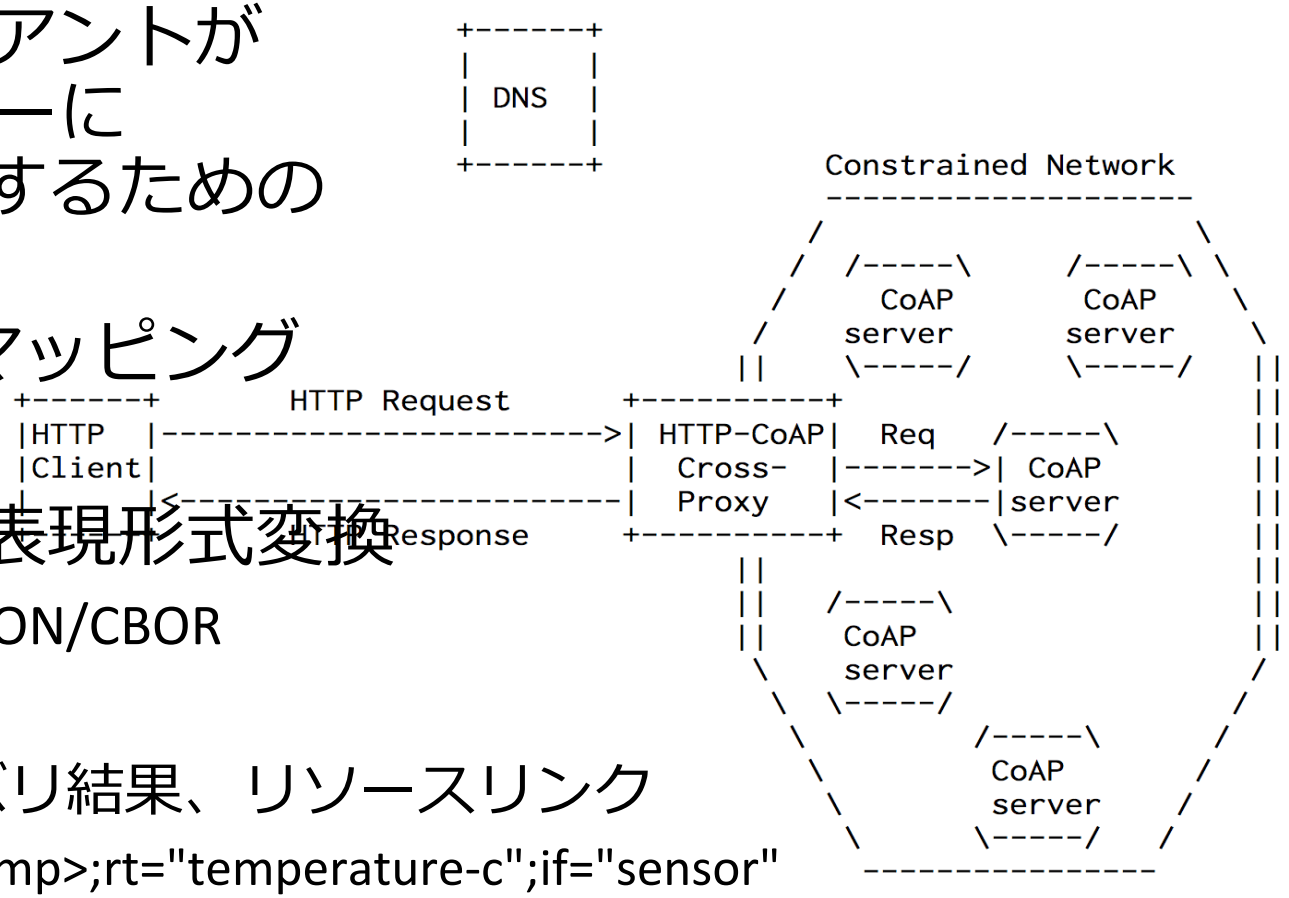


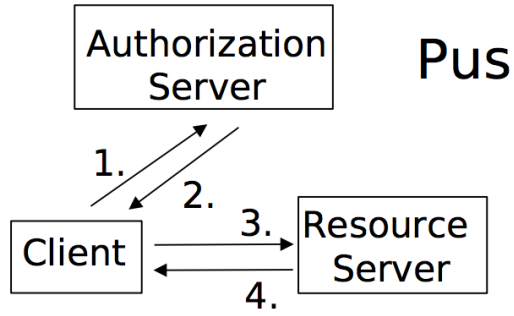
Figure 1: Reverse Cross-Protocol Proxy Deployment Scenario

ace WG (Wed July 23)

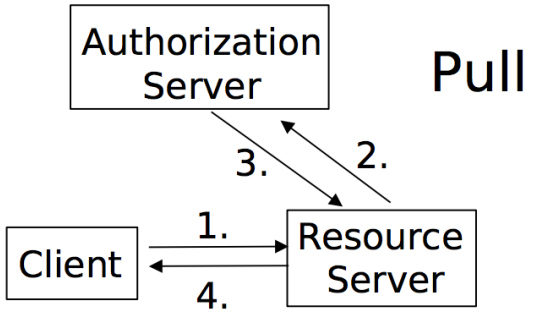
- Authentication and Authorization for Constrained Environments
  - 制限された環境での認証・認可
- SECエリアのWGとなって第1回目
  - 前回ロンドンではAPPエリアのBoF
- problem description, use cases, architectureを検討
  - Client (C), Resource Server (RS): 制約あり
  - Authorization Server (AS): 制約なし
  - boot-strapping: 当面考えない

ace Authorization Model

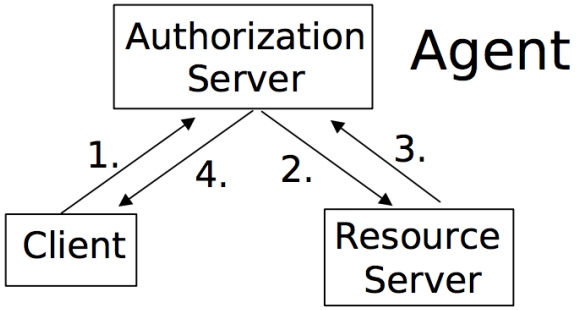
- AS – *Authorization Information* → RS (cf. RFC 2905)

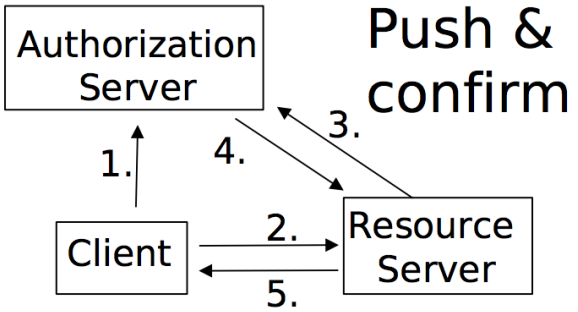


e.g. OAuth, Kerberos



e.g. EAP, ABFAB





e.g. OAuth token introspection

http://www.ietf.org/proceedings/90/slides/slides-90-ace-1.pdf

ace Problem Description

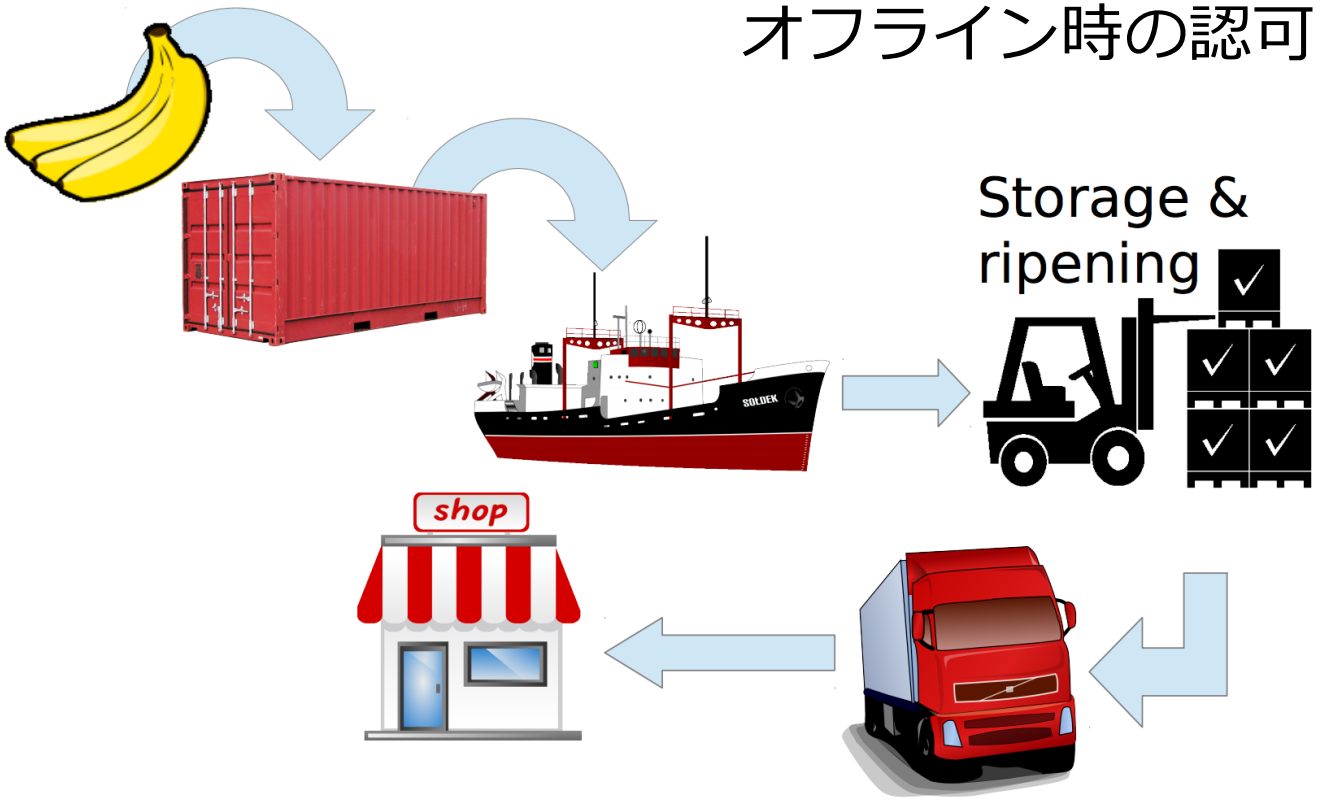
- http://www.ietf.org/proceedings/90/slides/slides-90-ace-1.pdf
- commSec
  - 通信路(DTLS)、オブジェクト(JWS/JWE)、hybrid
- Authorizationモデル
  - C,RS,ASの3-partyですべてのユースケースをカバーできるか?
  - RSからredirectによってASへ誘導するパターンも
  - ASは常にCを認証しないといけない
  - C - RS 間は常に相手を認証しているのか?
    - cf. 照明制御

ace Use Cases and Design Pattern

- http://www.ietf.org/proceedings/90/slides/slides-90-ace-2.pdf
- 4つのユースケースを考える
  - コンテナモニタリング
  - ホームオートメーション
  - ビルディングオートメーション
  - スマートメーター
- 前述のauthorization modelはどうか検討

ace Use Cases

Container Monitoring



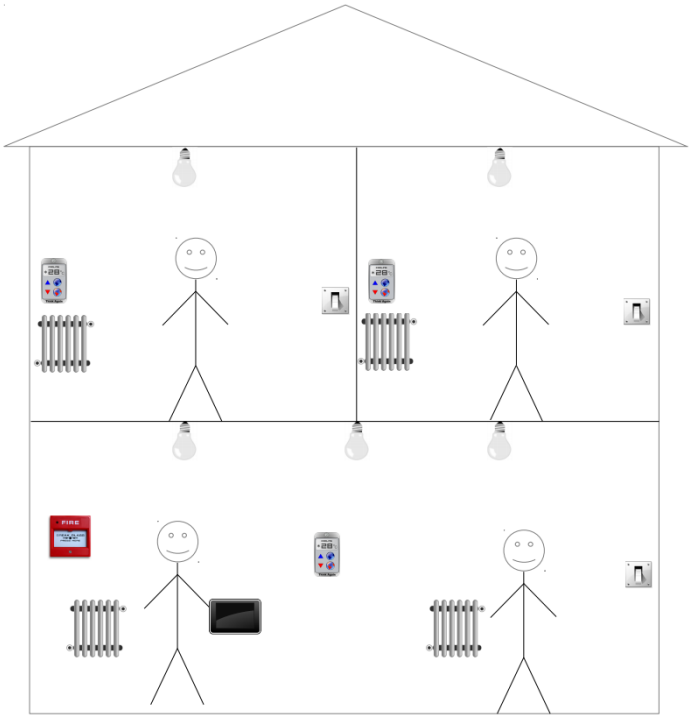
ace Use Cases

Home Automation

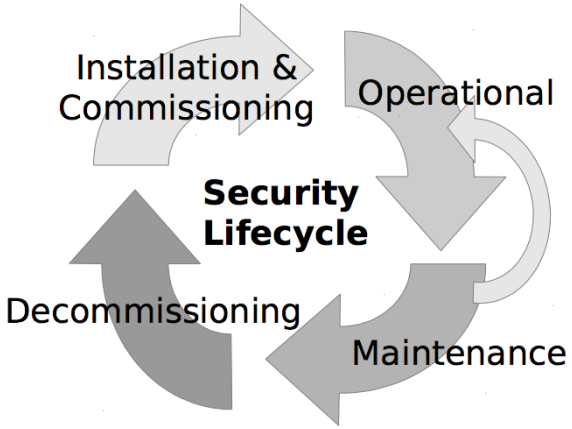
アクセス権のリモート委譲

ace Use Cases

Building Automation

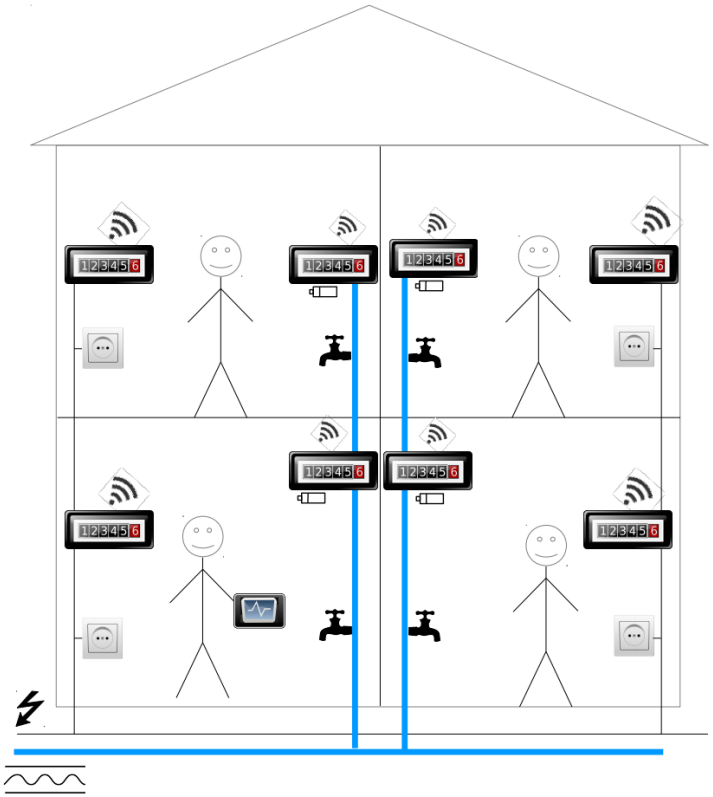


セキュリティー
ライフサイクル



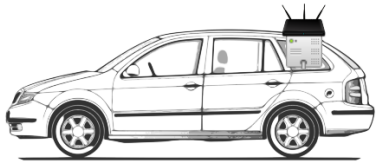
ace Use Cases

Smart Metering



電力センサーへの
水・ガスの相乗り

Base station



ace その他

- Design Considerations
  - http://www.ietf.org/proceedings/90/slides/slides-90-ace-3.ppt
  - 再利用可能なコンポーネントは?
    - 認可情報の内容/表現方法/検証/入手時期
    - 鍵とcipher suites
  - メッセージを小さく/少なく/省計算コスト
  - cryptoは対称 or 非対称?
    - コードサイズ、メモリ使用量
- Cross-Domain Support
  - C と RS が別のsecurity domainにいる場合の検討
  - 制限デバイスをサポートする非制限アクター

dice WG (Tue Jul 22)

- DTLS In Constrained Environments
- IoT向けDTLS profile
  - CoAP通信のセキュリティーはDTLSを使用
  - 認証/共通鍵/公開鍵/証明書ハンドリング

dice WGの話題

- DTLS profile
  - 証明書チェーンの最長深さ → 4をレコメンド
  - Constrained client - cloud server以外の組合せは後回し(aceの結果を待つ)
- Group Security(複数デバイス間の認証)
  - ユースケース不足
  - smart energy以外の用途
- Multicast (照明の一括操作など)
  - 共通/公開鍵ベースの署名検証などを検討

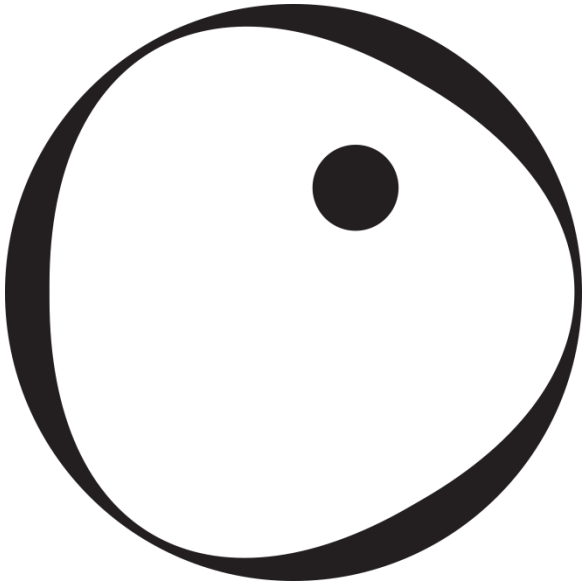
その他

- jose WG (Javascript Object Signing and Encryption)
  - JSON Web Token (JWT/JWS/JWE)
    - JSONをbase64urlエンコード
    - ヘッダ、クレームラベル定義 (alg, iss, sub, exp, iat)
    - 署名、暗号化
  - CBORでJWT同様のこと考える → COSE
    - base64は必要ない
    - よく使うラベル名はコード化
  - 今回はno action

まとめ

- IoTの標準化が進んでいる
  - ユースケース募集中
  - problem descriptionは手さぐり
- IETF90 Wrap Up - An Interview with IETF Chair Jari Arkko
  - http://www.youtube.com/watch?v=uzYS79jj7-o
  - IETF ChairがWrap Upの冒頭でIoTについて言及
- セキュリティとプライバシーのIoTへの取り組みが急速に増えている
  - Identityという単語がよく聞かれた

Any Questions? / Please Feedback!



lepidum

https://lepidum.co.jp/

mailto:maeda@lepidum.co.jp / twitter: @mad_p