信頼される安心を、社会へ。
SECOM

Hackathon と SUIT 報告
IoTファームウェア更新に関する議論

2019年5月17日

瀧田悠一
セコム株式会社　IS研究所

目次

信頼される安心を、社会へ。
SECOM

- IETF Hakathonへの参加
- Hackathon SUITプロジェクトでの活動
- IETF 104でのSUITの動向
- まとめ

目次

- IETF Hakathonへの参加
- Hackathon SUITプロジェクトでの活動
- IETF 104でのSUITの動向
- まとめ

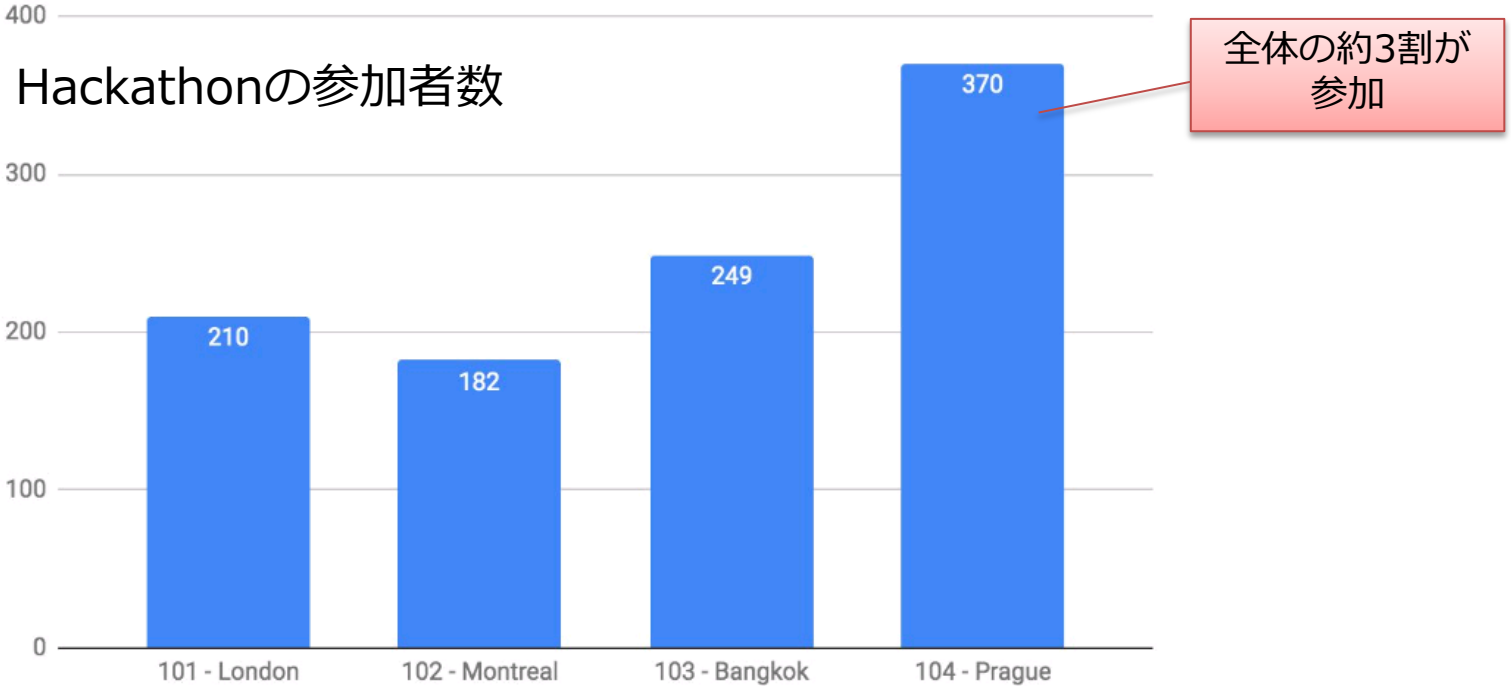
IETF Hackathon とは

- 概要
  - IETF標準の実装について、参加者による共同開発や議論を行うイベント
- 開催の目的
  - IETFの標準化活動の加速
  - IETFの活動への関心を広げるため
- 特徴
  - IETF 92から開催され、今回で13回目
  - IETFの始め2日間で実施（土、日）
  - 参加者はプロジェクトを選択して参加
  - 主にプロトコルの実装や相互運用性の検証に取り組む

出典：「Hackathon Photos」https://drive.google.com/drive/folders/14Ct_NQ7vJz7d1WIoER4Vrkmdx7sBTV59

Hackathon への関心の高まり

- IETF 104では、44プロジェクトが実施され、370人が現地参加
  - 会場の人口密度が高い！



出典：「IETF 014 Plenary」 https://datatracker.ietf.org/meeting/104/materials/slides-104-ietf-sessa-ietf-chair-slides-01

Hackathon への参加方法

信頼される安心を、社会へ。
SECOM

1. IETF Hackathonに参加登録
   - IETFのWebページ上で「Hakcathon Registration」を行う
   - 登録された参加者は「Hackathon Attendance」に掲載される

2. 参加したいプロジェクトを選ぶ
   - 「Hackathon wiki」のプロジェクト一覧や、Hackathonのメーリングリストから探す
   - プロジェクトの主催者（Champion）になることも可能

3. プロジェクトのChampionに参加希望を連絡
   - Hackathonで取り組みたいことを事前に伝える（メールでの連絡、会場で直接話す）

4. しっかりと準備をして参加！
   - 参加すると非常に勉強になる（ただし、予習は必須）
   - 最新のI-Dやメーリングリストでの議論の動向などを理解しておく

Hackathon 当日の流れ（1日目）

- Saturday, March 23
  - 08:30: Room open for setup by project champions
  - 09:00: Room open for all
  - 09:30: Hackathon kickoff
  - 09:45: Form Teams
  - 12:30: Lunch provided
  - 15:30: Afternoon break
  - 19:00: Dinner provided
  - 22:00: Room closes

出典：「IETF 104 Hackathon」 https://trac.ietf.org/trac/ietf/meeting/wiki/104hackathon

Hackathon 当日の流れ（2日目）

- Sunday, March 24
  - 08:30: Room opens
  - 12:30: Lunch provided
  - 13:30: Hacking stops
  - 14:00: Project presentations
  - 15:45: Closing remarks
  - 16:00: Hackathon ends
  - 17:00: Tear down complete

出典：「IETF 104 Hackathon」 https://trac.ietf.org/trac/ietf/meeting/wiki/104hackathon
右の写真の出展：「Hackathon Photos」https://drive.google.com/drive/folders/14Ct_NQ7vJz7d1WIoER4Vrkmdx7sBTV59

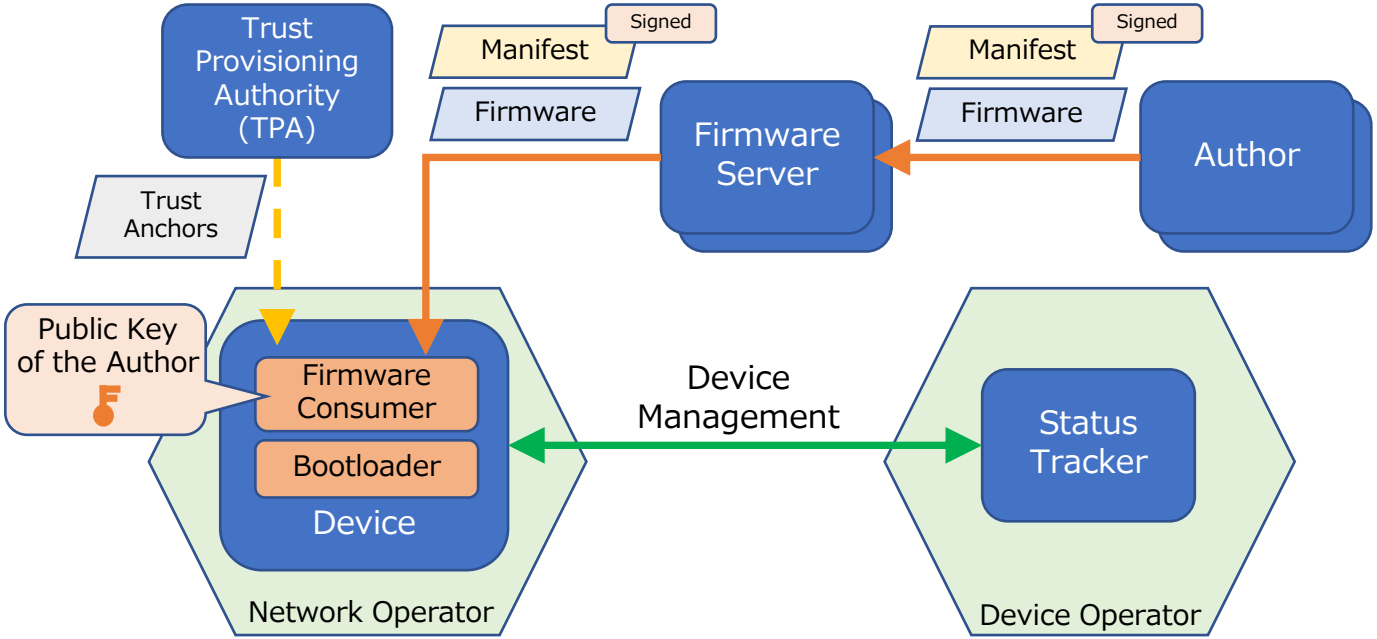
目次

信頼される安心を、社会へ。
SECOM

- IETF Hakathonへの参加
- Hackathon SUITプロジェクトでの活動
- IETF 104でのSUITの動向
- まとめ

SUIT（Software Updates for IoT）WGとは

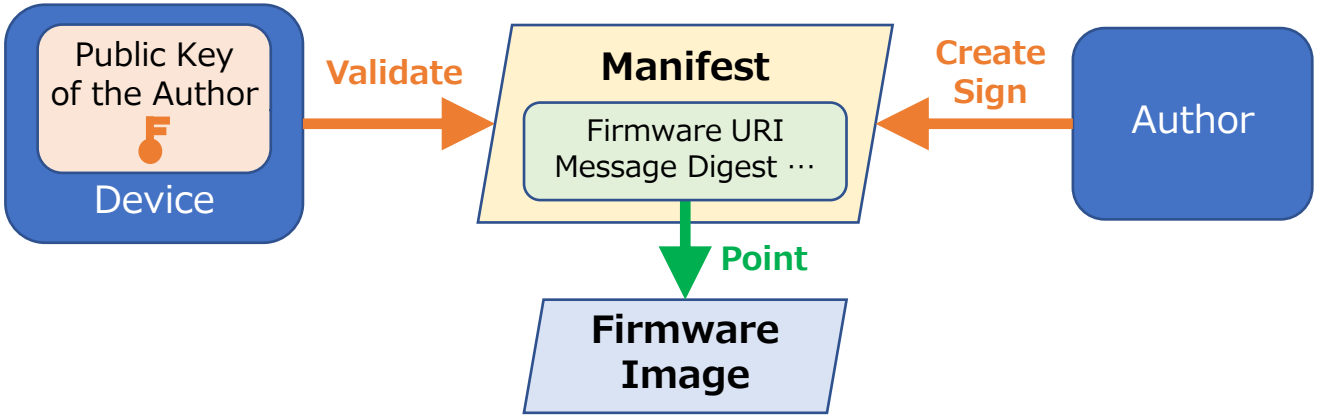
- IoT機器の安全なファームウェア更新の仕組みを検討
- Constrained Devices(～10KiB RAM, ～100KiB ROM)を目標



出典：「A Firmware Update Architecture for Internet of Things Devices」 https://tools.ietf.org/html/draft-ietf-suit-architecture

SUITの主要なドラフト

- draft-ietf-suit-architecture
  - SUITのアーキテクチャを定義（ARMなど）
- draft-ietf-suit-information-model
  - マニフェストの情報モデルを定義（ARM、Fraunhoferなど）
- draft-moran-suit-manifest
  - CBOR/COSEを使用したマニフェストフォーマットを定義（ARM、Fraunhoferなど）



SUITプロジェクトの参加者

信頼される安心を、社会へ。
SECOM

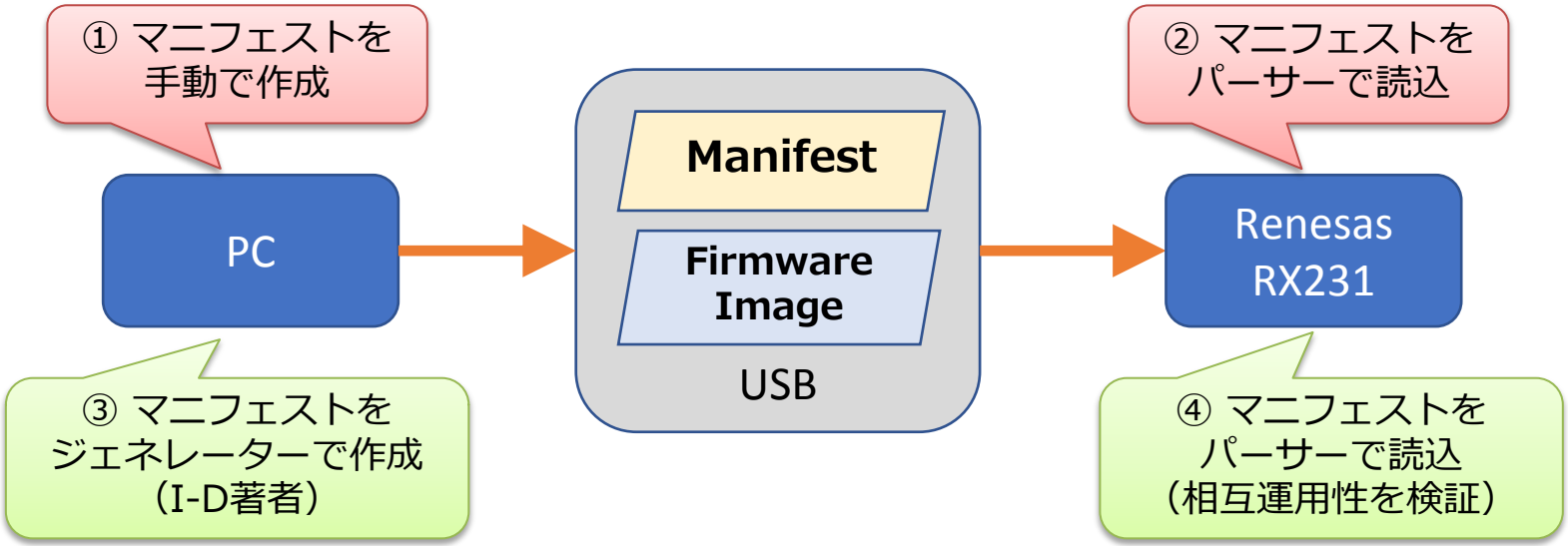
- 今回は12名が参加（前回が10名、前々回が8名）

マニフェストの
I-D著者も参加

出典：「Hackathon Report」 https://datatracker.ietf.org/meeting/104/materials/slides-104-suit-hackathon-report-01

SUITプロジェクトの目標

- 最新フォーマットに準拠するマニフェストの相互運用性を検証
  - ① マニフェストのジェネレーターの作成　⇒　I-D著者が担当
  - ② マニフェストのパーサーの作成　⇒　我々や他参加者が担当



SUITプロジェクトの結果

信頼される安心を、社会へ。
SECOM

- **manifest generators!**
  - 2 independent implementations (ARM, Renesas)
- **manifest parsers!**
  - 3 independent implementations (Inria/FUB, ARM, Renesas)
    - 2 of which running on small micro-controllers

Microchip SAMR21
Cortex-M0+
32kB RAM, 256kB ROM

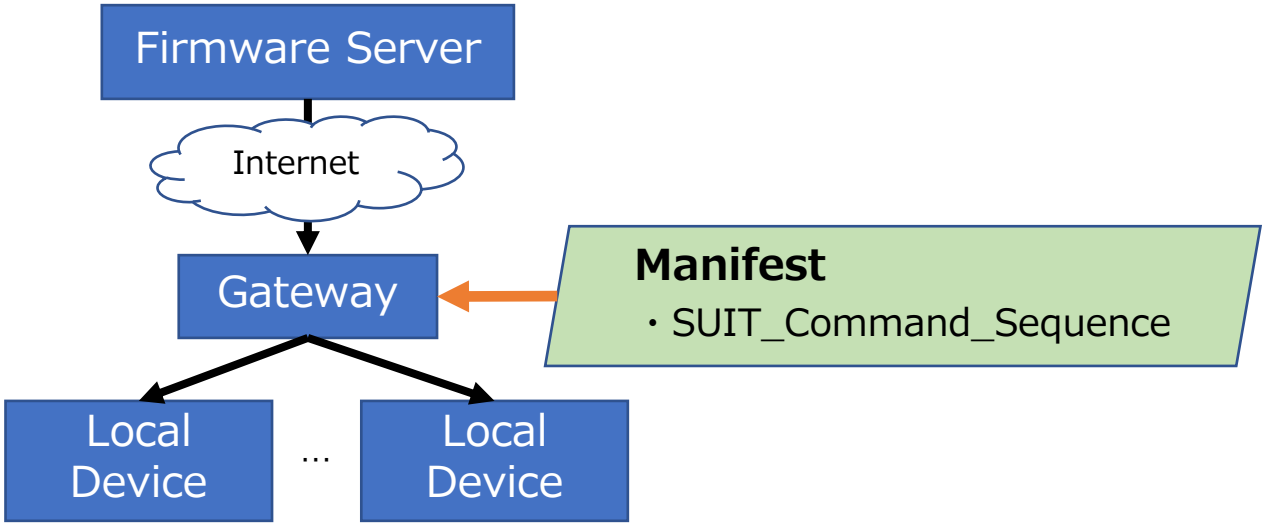
Renesas
Starter Kit
RX231
64kB RAM

- **interoperability!**
  - manifest generator (ARM) <=> parsers from Inria/FUB & Renesas
- **end-to-end workflow demo!**
  - (experimental) open source implementation based on RIOT

出典：「Hackathon Report」 https://datatracker.ietf.org/meeting/104/materials/slides-104-suit-hackathon-report-01

Hackathonでの意見交換

- マニフェストの項目のセマンティクスを確認
  - Component IDなど
- 具体的なExampleが必要なマニフェストがあることを提案
  - ファームウェア更新の手順を記述するケース



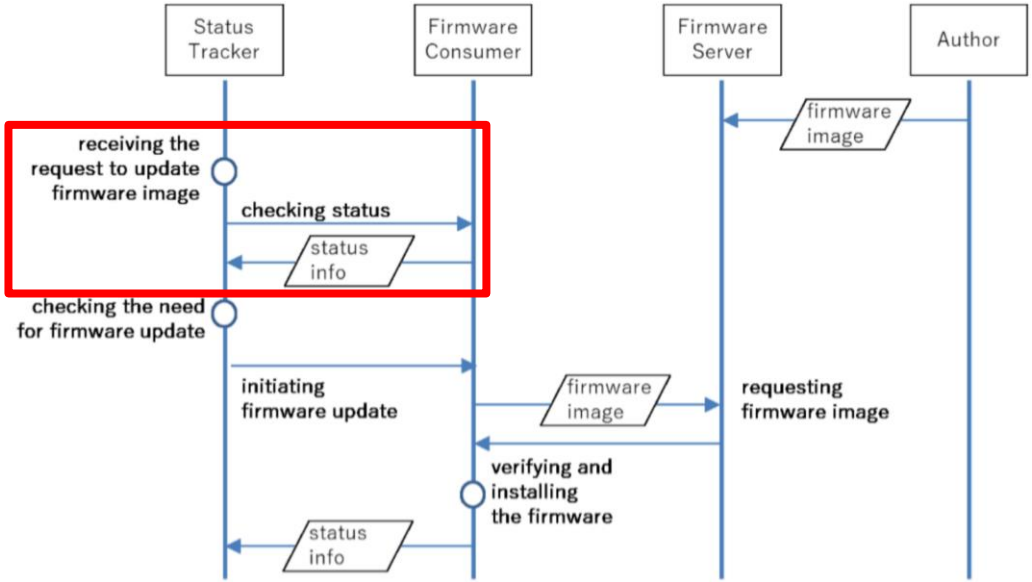
目次

信頼される安心を、社会へ。
SECOM

- IETF Hakathonへの参加
- Hackathon SUITプロジェクトでの活動
- IETF 104でのSUITの動向
- まとめ

動向① ITU-T SG17との協調

- SG17からのリエゾンステートメントへの対応
  - ITU-T X.secup-iotが改訂されたため、SUIT WGに確認を依頼
  - Status Trackerの役割に多少の差異があることなどを確認



出典：「Liaison statement from ITU-T SG17」 https://datatracker.ietf.org/meeting/104/materials/slides-104-suit-itu-t-sg17-liaison-statement-review-00.pdf

動向② WGドラフトの進捗

- Architecture と Information Model のI-Dが WG Last Callに向かうことについて確認

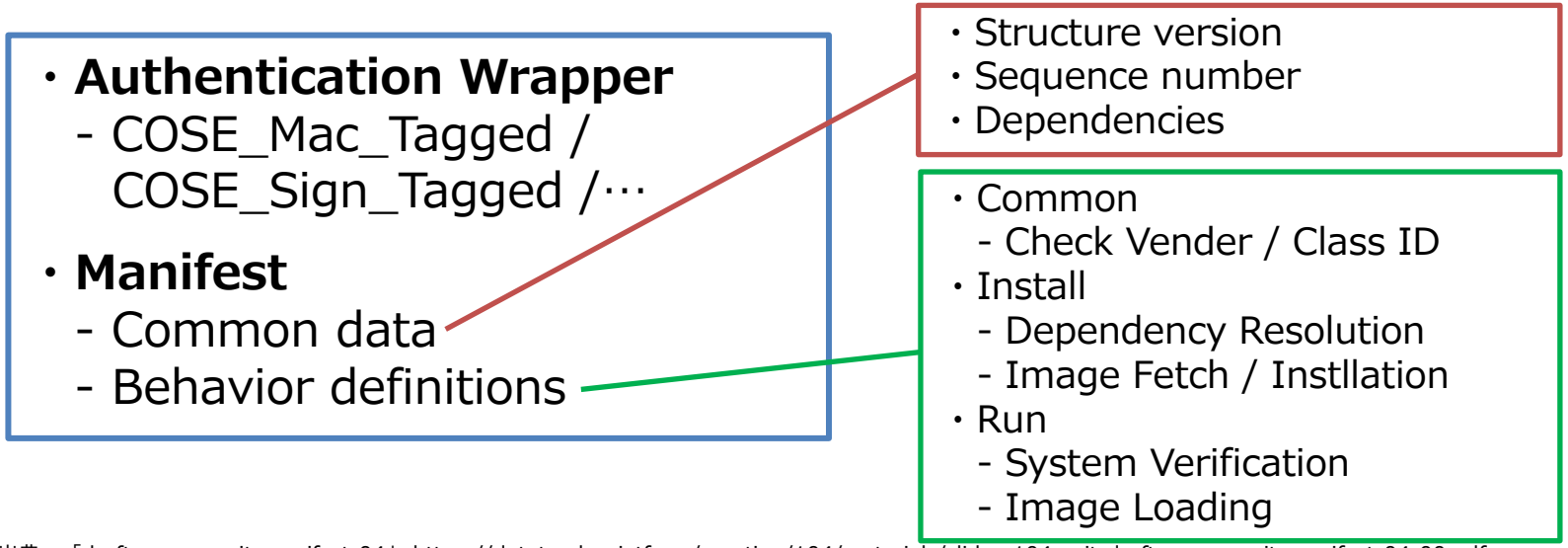
- draft-ietf-suit-architecture
  - 即座にWGLC

- draft-ietf-suit-information-model
  - エディトリアルな修正を加えた上でWGLC

動向③ マニフェストフォーマットの更新

信頼される安心を、社会へ。
SECOM

- 前バージョンのフォーマットは複雑だった
  - パーサーの実装が複雑化　⇒　コードサイズの増加
- 最新のフォーマットでは、構造を単純化しつつ、表現力を強化
  - 更新の条件や、コマンドが記述可能



出典：「draft-moran-suit-manifest-04」 https://datatracker.ietf.org/meeting/104/materials/slides-104-suit-draft-moran-suit-manifest-04-00.pdf

動向③ マニフェストの具体例

信頼される安心を、社会へ。
SECOM

- Download / Install, Verify compatibility, Secure boot
- Information (106 bytes)
  - Structure version : 1
  - Sequence Number : 2
  - Component ID : [h‘466c617368’, h‘013400’]
    - Translates to address 0x013400 in Flash.
    - 11 bytes
  - Size : 34768
  - Digest : SHA-256 (32 bytes)
  - URI : http://example.com/file.bin (27 bytes)
  - Device Class : 1492af14-2569-5e48-bf42-9b2d51f2ab45 (16 bytes)
  - Vendor ID : fa6b4a53-d5ad-5fdf-be9d-e663e4d41ffe (16 bytes)
- Encoded Size : 177 bytes

出典：「draft-moran-suit-manifest-04」 https://datatracker.ietf.org/meeting/104/materials/slides-104-suit-draft-moran-suit-manifest-04-00.pdf

他WGとの関連① TEEP

- 課題：TAに関する依存関係の表現方法
  - 「UA – TA間」、「TA - TA間」の依存関係
  - TAMによるソフトウェアの更新では依存関係を考慮する必要がある

- ChairよりSUITと互換性を持たせたいとの意見
  - 依存関係の表現にマニフェストを利用
  - 他のWGがマニフェストの定義を拡張

- 議論から予想される今後の課題
  - UAの更新に応じて、対応バージョンのTAを取得し更新する手続きの表現
  - 複数のUAのうち、あるUAだけが特定バージョンのTAを必要とする場合
  - TA1 → TA2 → TA3 といった順序性のある依存関係の表現

他WGとの関連② RATS

- 課題：EATに含まれるClaimの定義
  - ソフトウェアコンポーネントに関するClaim
  - 特に、そのサブモジュールやネスト構造の定義

- SUITのマニフェストが議論に出る
  - UEID(Universal Entity ID)にSUITのUUIDが参考になるとの意見
  - Vendor ID = UUID5 (DNS_PREFIX, vendor domain name)
  - Class ID = UUID5 (Vendor ID, Class-Specific-Information)

目次

- IETF Hakathonへの参加
- Hackathon SUITプロジェクトでの活動
- IETF 104でのSUITの動向
- まとめ

Hackathon と SUIT 報告　まとめ

信頼される安心を、社会へ。
SECOM

- IETF Hakathonへの参加
  - Hackathonへの関心が高まっており、現地の参加者数は増加傾向
  - I-DやRFCの著者らとF2Fで意見交換が可能
- Hackathon SUITプロジェクトでの活動
  - 様々なIoT機器を対象とする相互運用性の検証（実装方法、コードサイズなどの共有）
  - 特定のシステム構成での課題の共有、解決策の提案
- IETF 104でのSUITの動向
  - Architecture と Information Model のI-DがWGLC
  - マニフェストの具体的なフォーマットは検討を継続
  - 他WG（TEEP、RATS）との連携が強まってきている