信頼される安心を、社会へ。
SECOM

IoT機器の安全なファームウェア更新 SUIT と Hackathon

2018年12月14日

瀧田悠一

セコム株式会社　IS研究所

今回の活動の一部は、一般社団法人情報通信技術委員会(TTC)による以下の助成を受けて行いました。
平成30年度「IoT/BD/AI時代に向けたデジュール及びフォーラム標準に関する標準化動向調査」調査者の募集
http://www.ttc.or.jp/j/info/topics/20180410/

目次

信頼される安心を、社会へ。
SECOM

- SUITとは
- Hackathon SUITプロジェクトへの参加
- IETF103でのSUITの動向
- まとめ

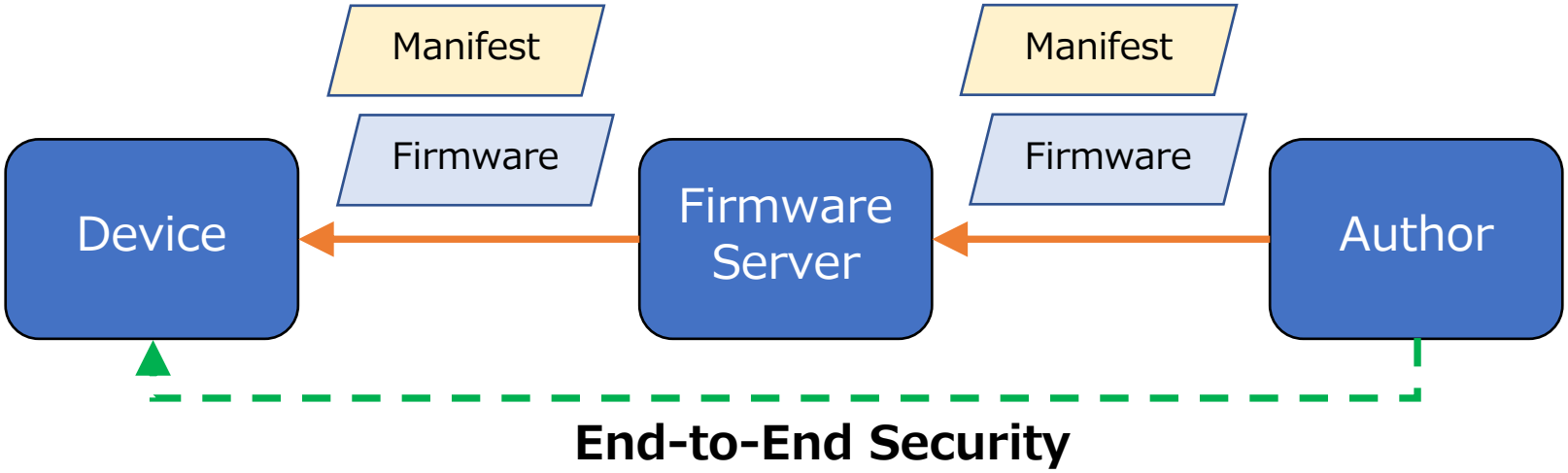
目次

信頼される安心を、社会へ。
SECOM

- SUITとは
- Hackathon SUITプロジェクトへの参加
- IETF103でのSUITの動向
- まとめ

SUIT WGとは

- Software Updates for IoTの略称
- 2017年に発足
- IoT機器の安全なファームウェア更新の仕組みを検討



SUITの特徴

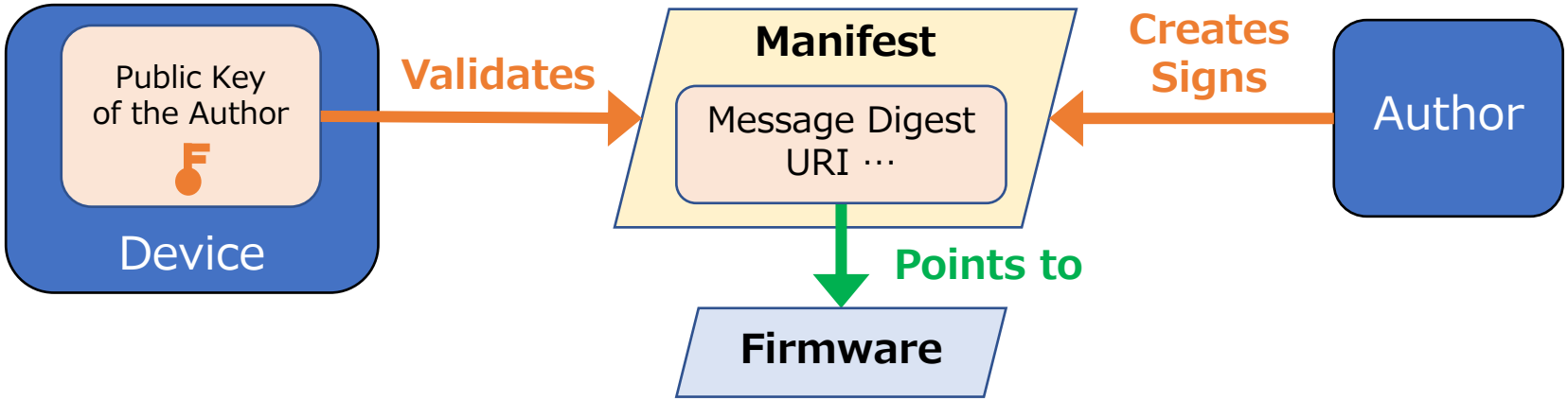
信頼される安心を、社会へ。
SECOM

- ファームウェアをEnd-to-Endで保護する仕組みであること
- 制限のある機器 (Constrained Devices) で動作することを重視
  - Class1 (~10KiB RAM、~100KiB ROM) が対象
- 既存のトランスポートプロトコルを使用する
- ファームウェア以外（例：PCのソフトウェア）の更新は対象外

End-to-Endのファームウェア保護

- ファームウェアの発行元を確認したい
  - ファームウェアはUSBメモリ、Wi-Fiなど多様な手段で配布される
  - 配布方法によっては安全ではない可能性がある

  -> デジタル署名を利用する



制限のある機器での動作： CBOR

- RFC 7049 Concise Binary Object Representation
- JSONをベースにしたバイナリのフォーマットを定義
- コードとメッセージのサイズが小さくなるように設計

JSON： 15bytes

[1,[2,3],[4,5]]

CBOR： 8bytes

```
83          # array(3)
   01       # unsigned(1)
   82       # array(2)
      02    # unsigned(2)
      03    # unsigned(3)
   82       # array(2)
      04    # unsigned(4)
      05    # unsigned(5)
```

出典：「Concise Binary Object Representation (CBOR)」 https://tools.ietf.org/html/rfc7049

制限のある機器での動作： COSE

- RFC 8152 CBOR Object Signing and Encryption
- CBORを利用したデジタル署名などのフォーマットを定義
- CBOR Tag
  - COSE_Sign ： 98 デジタル署名
  - COSE_Encrypt ： 96 暗号化データ
  - COSE_Mac ： 97 MAC（メッセージ認証符号）

出典：「CBOR Object Signing and Encryption (COSE)」 https://tools.ietf.org/html/rfc7049

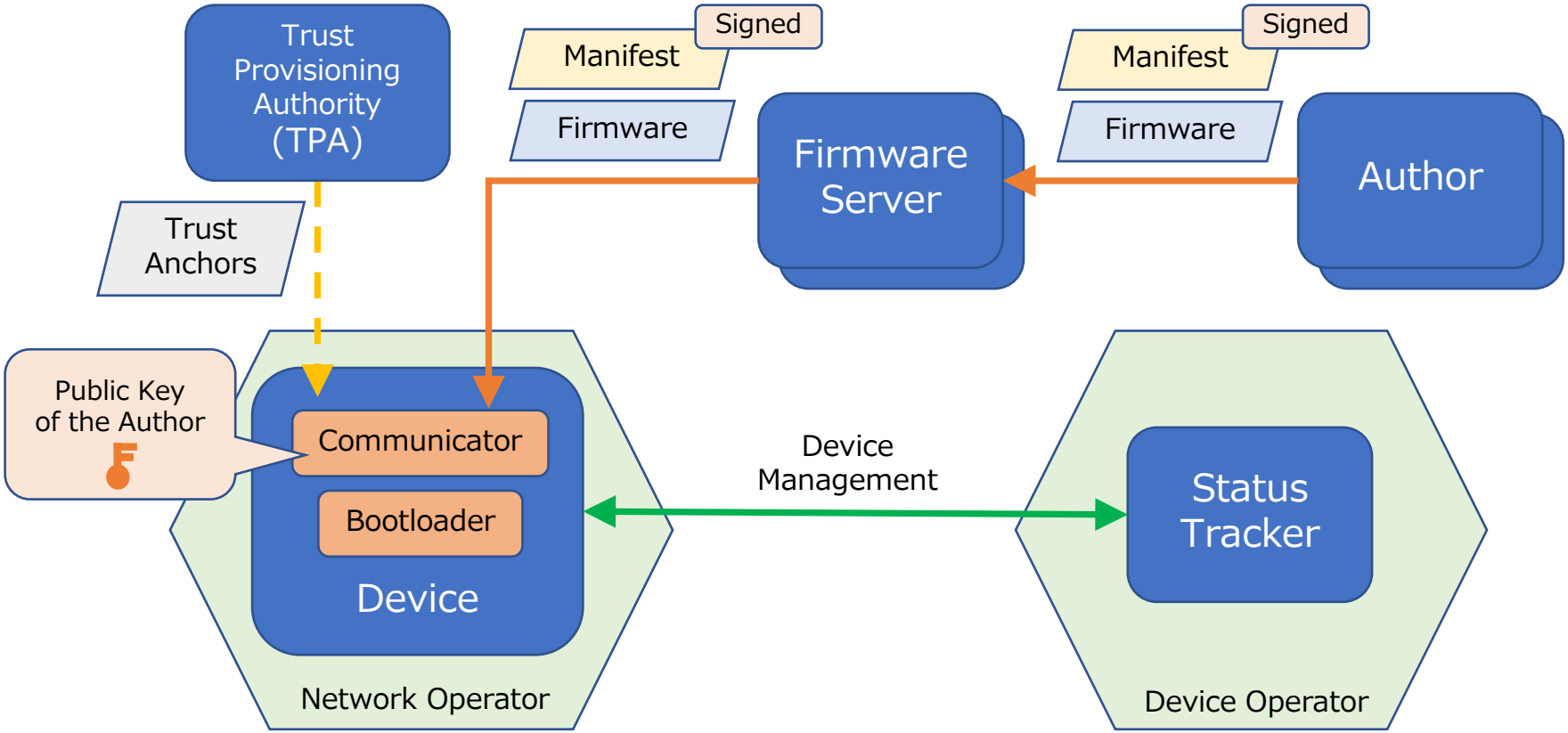
SUITのインターネットドラフト（I-D）

信頼される安心を、社会へ。
SECOM

- アーキテクチャと、マニフェストの情報モデル
  - A Firmware Update Architecture for Internet of Things Devices
  - Firmware Updates for Internet of Things Devices
    - An Information Model for Manifests

- マニフェストのフォーマット（3種類）
  - A CBOR-based Firmware Manifest Serialisation Format
  - Use of the Hash-based Signature Algorithm with CBOR Object Signing and Encryption (COSE)
  - A Binary Manifest Serialization Format

SUITのアーキテクチャ



出典：「A Firmware Update Architecture for Internet of Things Devices」 https://tools.ietf.org/html/draft-ietf-suit-architecture-01

マニフェストの例： 全体

信頼される安心を、社会へ。
SECOM

```
{
   / authenticationWrapper / 1 : 98([ 後述 ]),
   / manifest / 2 : { 後述 }
}
```

CBOR Diagnostic Notation による表記

map(2)

unsigned(1)

tag(98)

CBOR (バイナリ)

```
A201D8628444A103182AA0F6818343A10126A1045820537AC93AC909E79990914CAA00FE87E
EEA637EF89B5512E5CB6E558A136FF98D5847304502201D65938EC454354A6E866B468E9808
DB4EF36E97DE09F98FDA92E9C0E3302FC8022100AFF871FE581D3F6B831D74E46F9ACD7A015
E5548770B2A437970BE9272A7FBAA02A30101020105581A3018141300218250384686131303
1383239A0F658208CAF9283B13666CA4E50F7A1EEE86BA40B5E6A1D2CA39F7498B6A6A7BE8
D8D67
```

出典：「A CBOR-based Firmware Manifest Serialisation Format」 https://tools.ietf.org/html/draft-moran-suit-manifest-03

マニフェストの例： authenticationWrapper

```
/ authenticationWrapper / 1 : 98([
    / protected / h‘a103182a',
    / unprotected / {},
    / payload / null,
    / signatures / [[
        / protected / h‘a10126',
        / unprotected / {
            / kid / 4 : h‘537ac93a（略）136ff98d'
        } ,
        / signature / h‘30450220（略）72a7fbaa'
    ]]
])
```

{ / content type / 3 : 42 / application octet-stream / }

マニフェストの署名

{ / alg / 1 : -7 / ECDSA 256 / }

出典：「A CBOR-based Firmware Manifest Serialisation Format」 https://tools.ietf.org/html/draft-moran-suit-manifest-03

マニフェストの例： manifest

```
/ manifest / 2 : {
    / manifestVersion /  1 : 1,
    / sequence / 2 : 1,
    / payloads / 5 : [{
        / payloadComponent / 1 : [h'30'],
        / payloadSize / 2 : 37,
        / payloadDigest / 3 : [
            / protected / "a1011829",
            / unprotected / {},
            / payload /  null ,
            / tag / h‘8caf9283（略）be8d8d67'
        ]
    }]
}
```

ファームウェアのメッセージダイジェスト（COSE_Digest）

{ / alg / 1 : 41 / sha-256 / }

出典：「A CBOR-based Firmware Manifest Serialisation Format」　https://tools.ietf.org/html/draft-moran-suit-manifest-03

SUIT と Hackathon

信頼される安心を、社会へ。
SECOM

- 実際の機器では、ハードウェアやOSによって実装や動作が異なる
  - ハードウェアの性能やOSの機能によって違いがあるため
- SUIT WGでは IETF 101 Hackathonより参加し、結果をWGにフィードバックしてきた
- IETF 103でもSUITプロジェクトが参加することをうけて、我々も参加

目次

信頼される安心を、社会へ。
SECOM

- SUITとは
- Hackathon SUITプロジェクトへの参加
- IETF103でのSUITの動向
- まとめ

Hackathonの概要

- 2018年11月3日（土）～4日（日）の2日間開催
- 28プロジェクト、現地参加者は250人（IETF103現地参加者全体の約3割）
- SUITプロジェクトの参加者は10人、半数がHackathon初参加者

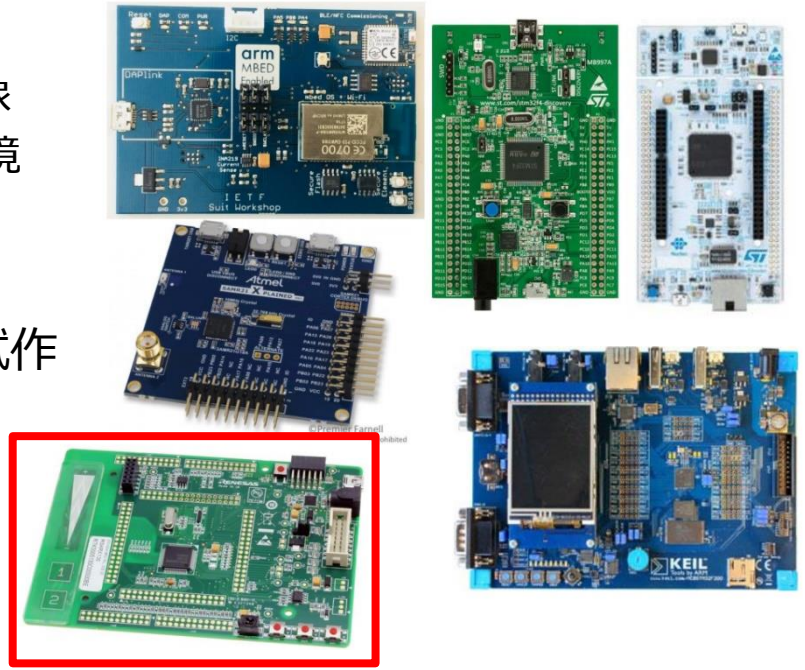
TEEPプロジェクトの方
(WG Chair) も同席

出典：「IETF Hackathon: Software Updates for IoT (SUIT)」　https://datatracker.ietf.org/meeting/103/materials/slides-103-suit-hackathon-report-00

SUITプロジェクトの目標

1. 仮想化されたSUIT開発環境の整備
   - IoT機器向けOS (Mbed OS、RIOT OS) を対象
   - SUITの開発に必要な環境を整備した仮想化環境 (Dockerコンテナ) を構築

2. 最新版のマニフェストフォーマットによる試作
   - 6つのハードウェア (HW) で試作
   - PC：　マニフェストの作成
   - HW：　マニフェストのパーサーの実装・動作
   - 我々はルネサスエレクトロニクス社の RX231を使用



出典：「IETF Hackathon: Software Updates for IoT (SUIT)」　https://datatracker.ietf.org/meeting/103/materials/slides-103-suit-hackathon-report-00

トラブル発生： 電源

- 開発ボードのACアダプタが故障
  - 日本とタイの電圧の違い
- 現地の電気店でACアダプタを購入
  - プラグの形状が開発ボードのものと異なる
- 購入したACアダプタのプラグを古いものと換装
  - Hackathonの参加者から助言をいただき、プラグを換装

トラブル発生： インターネットドラフト

信頼される安心を、社会へ。
SECOM

- マニフェストフォーマットのスキーマ定義（CDDL*1）に誤りを発見
  - JSON形式のマニフェストからCBOR形式が自動生成できなくなった
- スキーマ定義の修正を待つと時間が不足
  - 参加者間で正しいスキーマ定義を共有しながら、手動で作成
- CBORのRFC著者の方などからも、助言をいただきながら作業
  - マニフェストの作成、および、RX231で動作するパーサーを実装できた

※1 CDDL： Concise data definition language

Hackathonで明らかになった課題 ①

信頼される安心を、社会へ。
SECOM

- RX231はファームウェアの暗号化に対応
  - 暗号化されたファームウェアと対応する鍵を用いて更新を行う
- Hackathonでは我々の試作だけがファームウェア暗号化に対応
  - 現在のマニフェストには鍵を特定する項目(鍵ID)がないことに気がつく
- SUIT、CBOR、COSEのメンバーらと意見交換し、鍵IDの課題を整理
  - 鍵IDがユニークであるか、に関する議論など

Hackathonで明らかになった課題 ②

```
/ manifest / 2 : {
    / manifestVersion /  1 : 1,
    / sequence / 2 : 1,
    / payloads / 5 : [{
        / payloadComponent / 1 : [h'30'],
        / payloadSize / 2 : 37,
        / payloadDigest / 3 : [
            / protected / "a1011829",
            / unprotected / {},
            / payload /  null ,
            / tag / h‘8caf9283（略）be8d8d67'
        ]
    }]
}
```

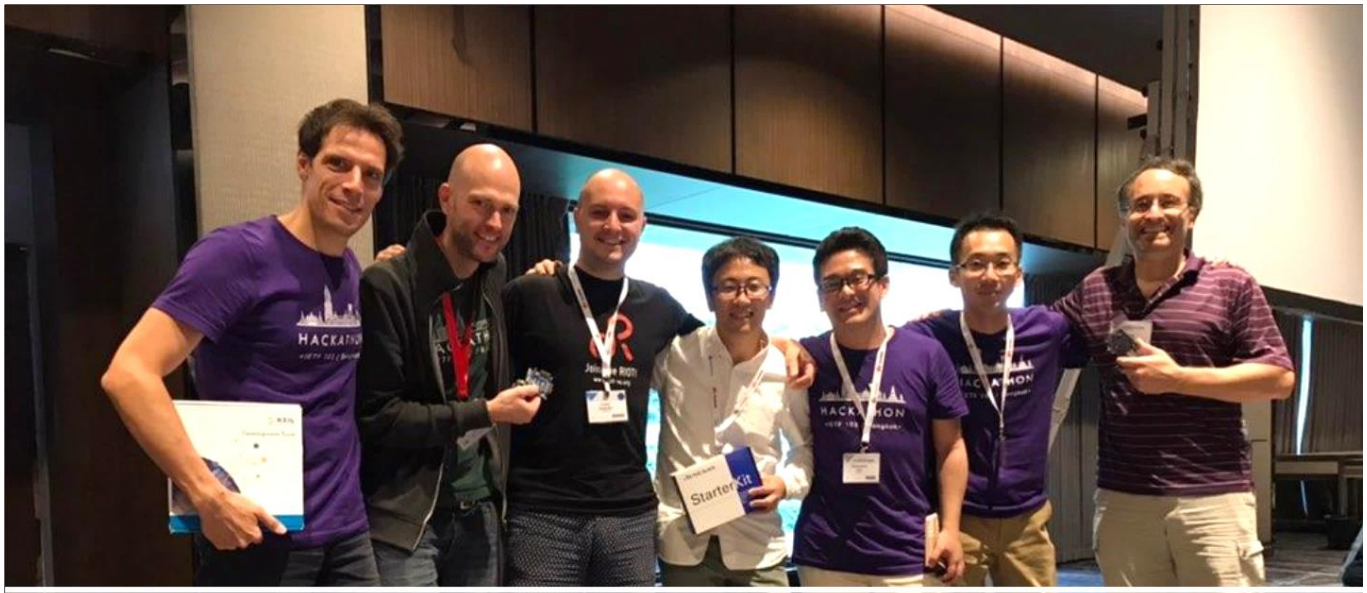
鍵ID（kid）の追加

出典：「A CBOR-based Firmware Manifest Serialisation Format」　https://tools.ietf.org/html/draft-moran-suit-manifest-03

ベストプロジェクトへの選出

信頼される安心を、社会へ。
SECOM

- Hackathonの2日目の午後に、各プロジェクトの代表者による成果発表が実施
- 参加者による投票の結果、SUITプロジェクトはベストプロジェクトに選ばれた



Yayy!! Software Updates for IoT (SUIT) was the winner at the #IETFHackathon #IETF103

出典：「IETF Hackathon: Software Updates for IoT (SUIT)」 https://datatracker.ietf.org/meeting/103/materials/slides-103-suit-hackathon-report-00

目次

- SUITとは
- Hackathon SUITプロジェクトへの参加
- IETF103でのSUITの動向
- まとめ

SUITの動向　ITU－T SG17との協調①

信頼される安心を、社会へ。
SECOM

- SG17からのリエゾンステートメントについて議論
- SG17が安全なソフトウェアアップデートに関するドラフトを作成中
  - ITU-T X.secup-iot (Secure software update for IoT devices)
- 用語の違い
  - Manifest、Author、Firmware Server、Status Tracker、 Firmware Consumer

SUITの動向　ITU－T SG17との協調②

信頼される安心を、社会へ。
SECOM

- WGへの質問
  - SG17の文書と一致するように、 SUITのアーキテクチャを更新するか？

    -> Yes

  - SG17の文章への参考引用を追加するべきか？

    -> SUITのアーキテクチャは協調している（aligned）と述べる

  - リエゾンステートメントにレスポンスするか？

    -> ミーティングにITU参加者がいるため不要

SUITの動向　マニフェストフォーマットの数①

信頼される安心を、社会へ。
SECOM

- 3種類のフォーマットをいくつに絞り込むか、について議論
  - draft-moran-suit-manifest　　CBOR形式、Hackathonで使用
  - draft-birkholz-suit-coswid-manifest　　CBOR形式
  - draft-pagel-suit-manifest　　独自バイナリ形式

- 1つのCBOR形式は、もう片方に統合
  - 「draft-birkholz-suit-coswid-manifest」は「draft-moran-suit-manifest」にカバーされている、という認識が示された

SUITの動向　マニフェストフォーマットの数②

信頼される安心を、社会へ。
SECOM

- 残りのフォーマットに関する論点は、Class1機器での実装
  - コードサイズ：「署名の検証処理」と「マニフェストのパース処理」
  - パース処理に関する実装のオーバーヘッド

- 参加者の認識を知りたいということで Humを実施
  - 1つのフォーマットにするか？（Yes or No）、また情報が十分ではないか？
  - 「Yes」と「まだ情報が十分ではない」が半々、という結果になった

目次

- SUITとは
- Hackathon SUITプロジェクトへの参加
- IETF103でのSUITの動向
- まとめ

SUITとHackathon まとめ

信頼される安心を、社会へ。
SECOM

- IoT機器の安全なファームウェア更新は、セキュリティの継続的な確保に不可欠
  - 制限のある機器が更新できれば、安価なIoT機器が長期間運用できる
- Hackathonでは他の参加者と協力して、問題に対処
  - I-DやRFCの著者らとつながりを得ることができた
  - 特定環境でのI-Dの課題も、関係者と素早く共有できた
- Hackathonなどを通じて、相互運用可能な技術を検討することは重要
  - 共通化されたファームウェア更新のツールなどを様々なIoT機器で利用できるようになると期待