ICTビジネス戦略セミナー　第2回

IETFにおけるIoT関連技術の動向と今後の活動予定

2019年1月28日

伊藤　忠彦
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

- IETFにおけるIoT関連技術の動向
- SUIT WGの動向
- HackathonでのSUIT動向（IETF103）
- 今後の活動予定

IETFにおけるIoT関連技術の動向

IETFとは

- Internet Engineering Task Force
  - インターネット技術の標準を策定
  - ボランタリ
  - 投票でなく、参加者のラフコンセンサスを重視
  - Internet of Thingsもスコープ

IETFでのIoT関連技術

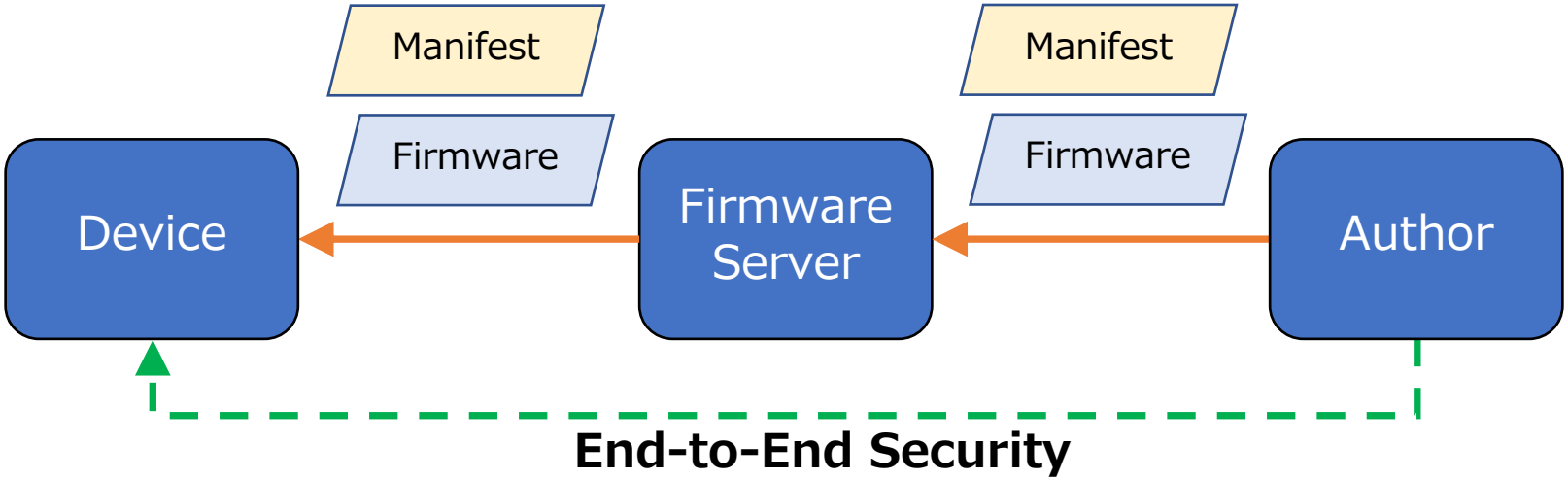
- 繋げる（ IoT機器向けの通信プロトコル）
  - L3以下の低レイヤ
    - 2005～2014 : 6LoWPAN (IPv6 over Low power WPAN) WG
    - 2013～ : 6lo (IPv6 over Networks of Resource-constrained Nodes) WG
    - 2013～ : 6TiSCH (IPv6 over the TSCH mode of IEEE 802.15.4e) WG
    - etc..
  - 高レイヤでの通信
    - 2010～ : CoRE (Constrained RESTful Environments ） WG
    - etc..
- 使う(IoT機器での認可など)
    - 2014～ : ACE (Authentication and Authorization for Constrained Environments) WG
    - etc..
- 管理する
  - 2017～ : SUIT（ Software Updates for Internet of Things) WG
  - 2019～? : RATS（ Remote ATtestation ProcedureS ） WG

サービスのオペレーションも絡んできた
弊社のビジネスにも近づいてきた

SUIT WG

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



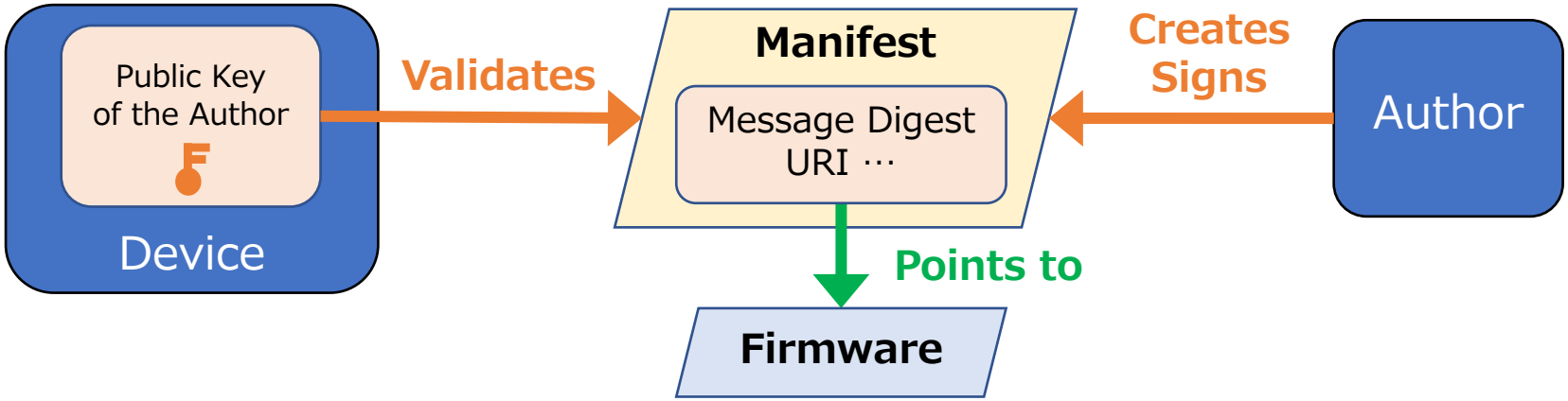
ＳＵＩＴの特徴

- 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

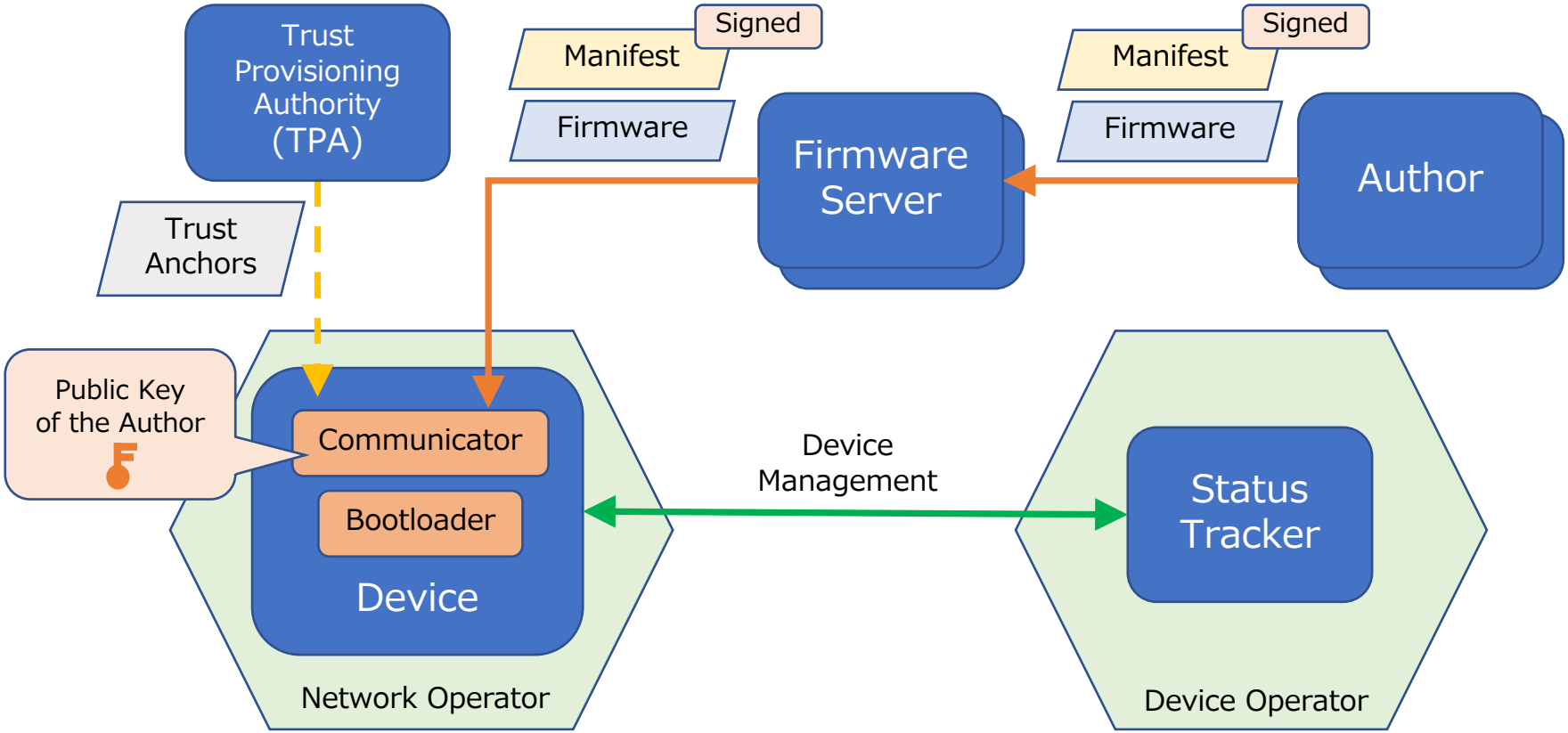
詳細資料はhttps://www.isoc.jp/wiki.cgi?page=IETF103Updateをご参照ください

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

詳細資料はhttps://www.isoc.jp/wiki.cgi?page=IETF103Updateをご参照ください

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

ＳＵＩＴとＨａｃｋａｔｈｏｎ

- 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の機能に違いがあるため
- SUIT WGでは IETF 101 よりHackathonを実施し、
  結果をWGにフィードバックしてきた
- IETF 103でもSUITプロジェクトが実施されることをうけて、
  我々も参加

HackathonでのSUIT WGの動向

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

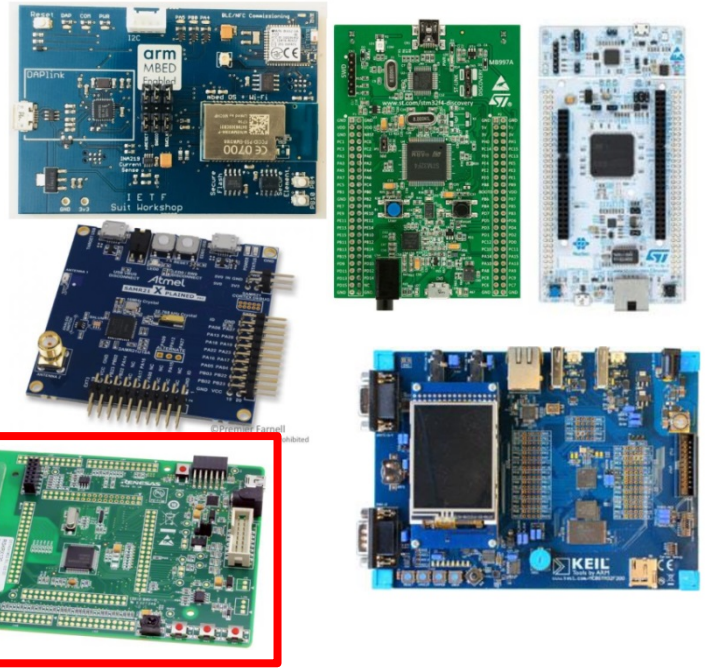
TEEPプロジェクトの方
(WG Chair) も同席

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換装
  - Hackathonの参加者から助言をいただき、換装に成功

トラブル発生：　インターネットドラフト

- 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

- 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

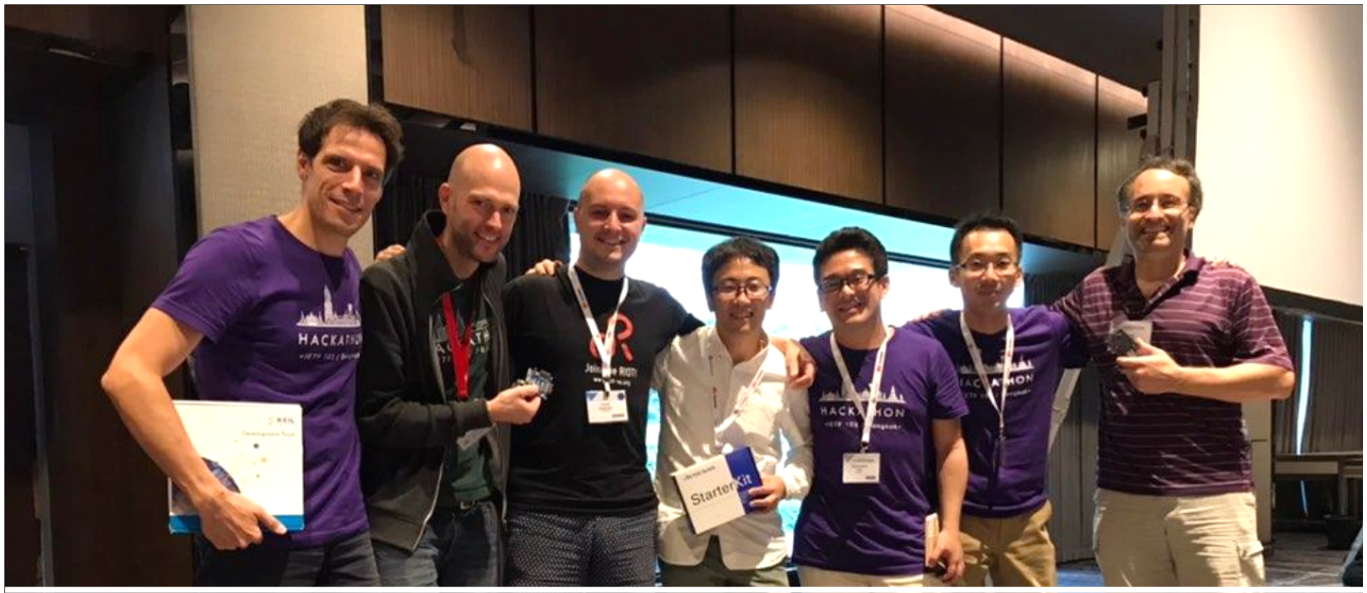
```
/ manifest / 2 : {
    / manifestVersion /  1 : 1,
    / sequence / 2 : 1,
    / payloads / 5 : [{
        / payloadComponent / 1 : [h'30'],
        / payloadSize / 2 : 37,
        / payloadDigest / 3 : [
            / protected / "a1011829",
            / unprotected / {},
            / payload /  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

- Hackathonの2日目の午後に、各プロジェクトの代表者が成果を発表
- 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

まとめと今後の活動

ＳＵＩＴとＨａｃｋａｔｈｏｎ　まとめ

- 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
  - ドキュメントを読んでも分からない事が分かってきた
  - 具体的な技術を把握するために一番の近道
  - 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
- 世界中の技術者が集まって議論して出した技術、相互運用可能な最新技術
  - 主導はArmなど
  - 国内動向とは、かい離があるように感じた
  - 日本語の詳細な資料もほとんど存在しなかった

IETFでのIoT関連技術

- 繋げる（ IoT機器向けの通信プロトコル）
  - L3以下の低レイヤ
    - 2005～2014 : 6LoWPAN (IPv6 over Low power WPAN) WG
    - 2013～ : 6lo (IPv6 over Networks of Resource-constrained Nodes) WG
    - 2013～ : 6TiSCH (IPv6 over the TSCH mode of
    - etc..
  - 高レイヤでの通信
    - 2010～ : CoRE (Constrained RESTful Environm
    - etc..
- 使う(IoT機器での認可など)
    - 2014～ : ACE (Authentication
    - etc..
- 管理する
  - 2017～ : SUIT（ Software Updates for Internet of Things)
  - 2019～? : RATS（ Remote ATtestation ProcedureS ）

よりサービスに近くなる
⇓
ローカライズ問題が出てくる（はず）
⇓
その時に取り残されないように

事前にインプットするのが一番労力が少ない。
事後だと、凄く苦労する

（IETFでの）今後の活動

- オペレーションに近づいてきた
  - より多くの機器が相互接続する流れは、今後も継続すると考えている

- 今後も最新動向について、広く情報公開していきたい
  - 国内動向や、日本の制度とのかい離が少なくなるように
  - 自分たちのやりたい環境での課題発見や共有も