信頼される安心を、社会へ。
SECOM

IoTセキュリティ関連

- データモデルと機器管理技術の標準化動向 -

2020年12月23日

瀧田悠一
セコム株式会社

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。
2020年度「デジュール及びフォーラム標準に関する国際標準化動向調査」調査者の募集
https://www.ttc.or.jp/topics/20200203

本日お話する内容

信頼される安心を、社会へ。
SECOM

① IoTデータモデルの標準化動向

- ASDF

② IoT機器管理技術の標準化動向

- SUIT / TEEP / RATS / MUD

③ 今後の動向

- IoT Operations WG

IETF ASDF WGの概要

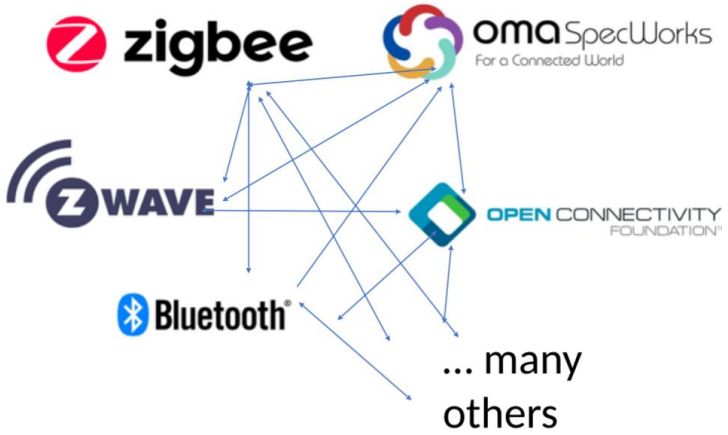
- **正式名**：**A** **S**emantic **D**efinition **F**ormat for Data and Interactions of Things
- **Area**　：Applications and Real-Time Area (art)
- **チェア**：Michael Richardson, Niklas Widell
- **経　緯**：
  - 2020年7月のIETF 108でBoFが開催（97人参加）
  - 議論に参加したいかどうかのhumでFORTISSIMO（有望な結果）
  - 10月にWGとして成立、11月のIETF 109でWG meeting開催
- **ASDFの目的**：
  - OneDM (One Data Model Liaison Group）が提案するIoTデータモデルのフォーマット仕様 SDF (Semantic Definition Format）の標準化

OneDM (One Data Model Liaison Group)とは

- **設立の経緯：**
  - 2018年秋、IoT産業の関係者が集まる**Zigbee**のミーティングで議論が開始
  - 共通のIoTデータモデルが存在していないことについて問題意識を共有
  - 2020年7月（IETF ASDF BoF開催と同時期）に活動を公開

- **現在の状態：**
  - 現在は複数のIoT関連SDO※とベンダーで構成されたメンバーで活動

※ Standards Development Organization



出典：https://datatracker.ietf.org/meeting/109/materials/slides-109-asdf-consolidated-slides-asdf-109-00

OneDMが解決したい課題

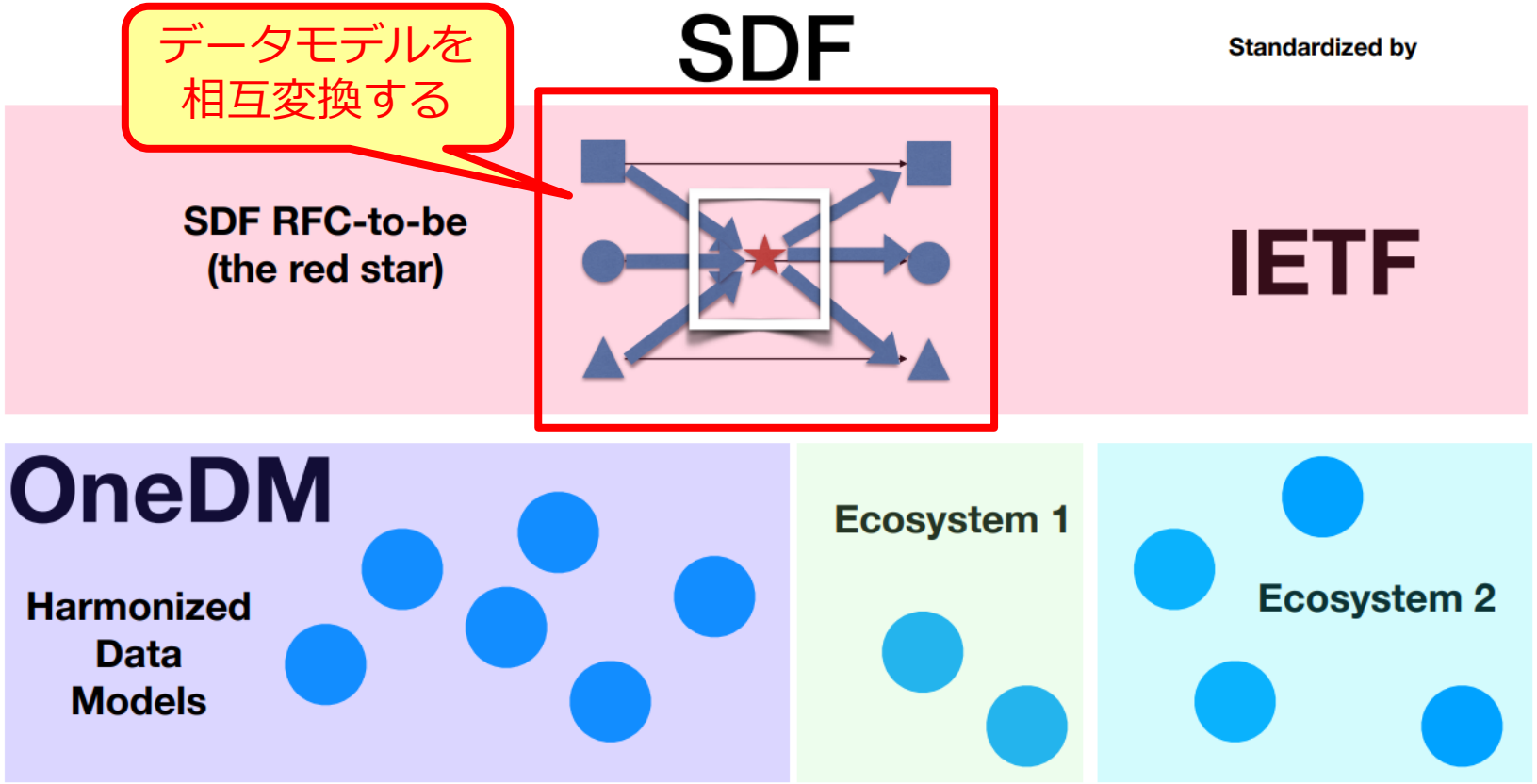
信頼される安心を、社会へ。
SECOM

- **IoTデータモデルの標準化：**
  - 現在、IoTデータモデルは各SDOが独自のメタモデルと表記方法を使用
  - 表記方法はそれぞれ異なるものの、メタモデルは概念的に非常に似ている
  - **業界全体で共通のIoTデータモデルが必要だが、既存のモデルでは不十分**
  - 既に存在するIoTデータモデルを相互変換するため、適切な抽象度の新しいデータモデルを記述する表記法が必要

⇒ OneDMはSDF（Semantic Definition Format）を定義

⇒ SDFをIETFでRFCとして標準化したい

SDFの位置づけ　- IETF and OneDM -

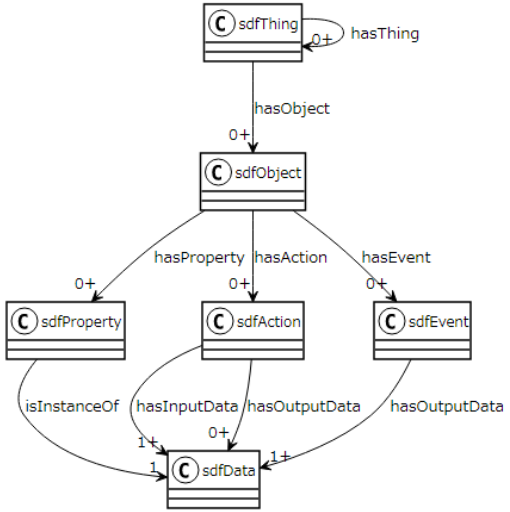


出典：https://www.ietf.org/proceedings/108/slides/slides-108-asdf-consolidated-slides-02

SDF(Semantic Definition Format)の概要

- SDFはJSONで記述するIoTデータモデルのフォーマット
  - 現時点では「**draft-ietf-asdf-sdf-01**」で定義
  - 表記方法にjson-schema.orgを一部引用
  - SDF自体の構文はCDDL (RFC 8610)で定義

- SDFはIoT機器（**Thing**）のデータモデルを定義する
  - SDFでは、モデルの最小構成要素を**Object**と呼ぶ



出典：https://onedm.org/SDF/sdf.html

- SDFのObjectは3つのAffordanceのタイプから構成されている
  - **Property**　：オブジェクトの状態の読み書き・使用に関するAffordance
  - **Action**　：オブジェクトに名前付きの操作を実行するためのAffordance
  - **Event**　：オブジェクトに何が起こったかの情報を取得するためのAffordance

SDFのExample - Switch -

信頼される安心を、社会へ。
SECOM

Object

Property

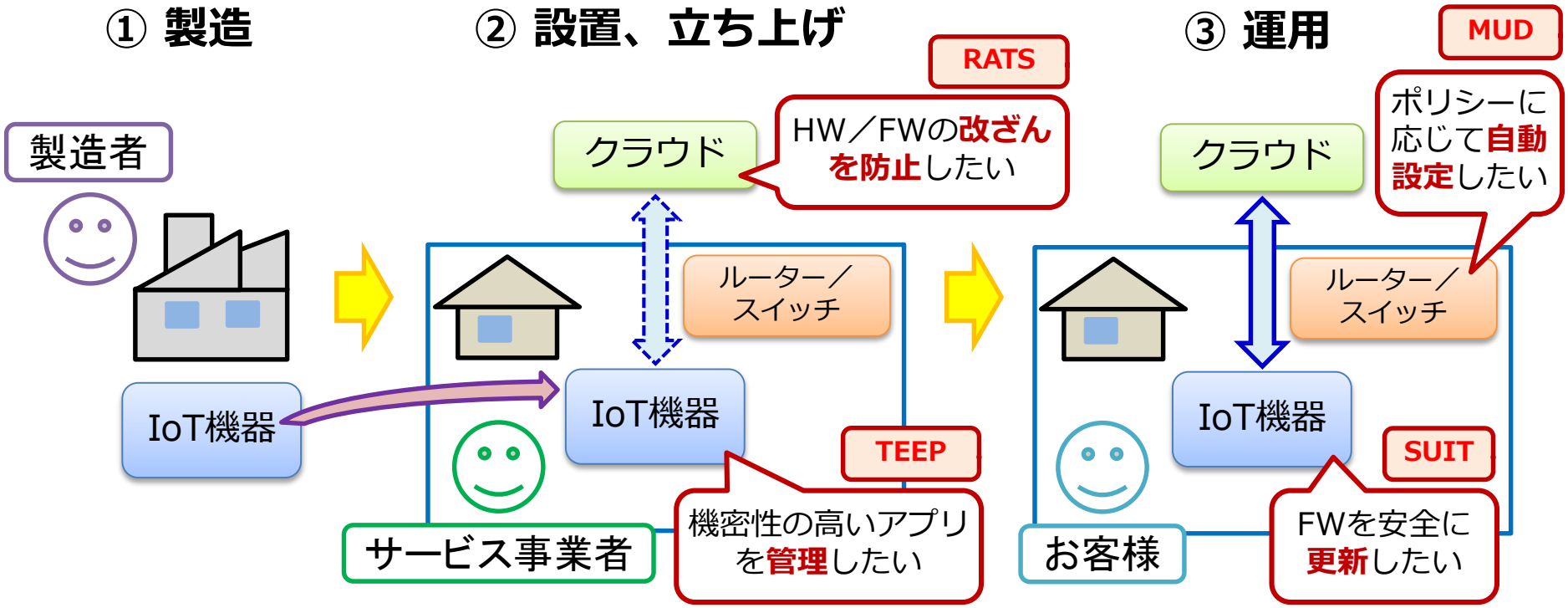
Action

```
{
    "info": {
        "title": "Example file for OneDM Semantic Definition Format",
        "version": "2019-04-24",
        "copyright": "Copyright 2019 Example Corp. All rights reserved.",
        "license": "https://example.com/license"
    },
    "namespace": {
        "cap": "https://example.com/capability/cap"
    },
    "defaultNamespace": "cap",
    "sdfObject": {
        "Switch": {
            "sdfProperty": {
                "value": {
                    "description": "The state of the switch; false for off and true for on.",
                    "type": "boolean"
                }
            },
            "sdfAction": {
                "on": {
                    "description": "Turn the switch on; equivalent to setting value to true."
                },
                "off": {
                    "description": "Turn the switch on; equivalent to setting value to false."
                },
                "toggle": {
                    "description": "Toggle the switch; equivalent to setting value to its complement."
                }
            }
        }
    }
}
```

出典：https://tools.ietf.org/html/draft-ietf-asdf-sdf-01

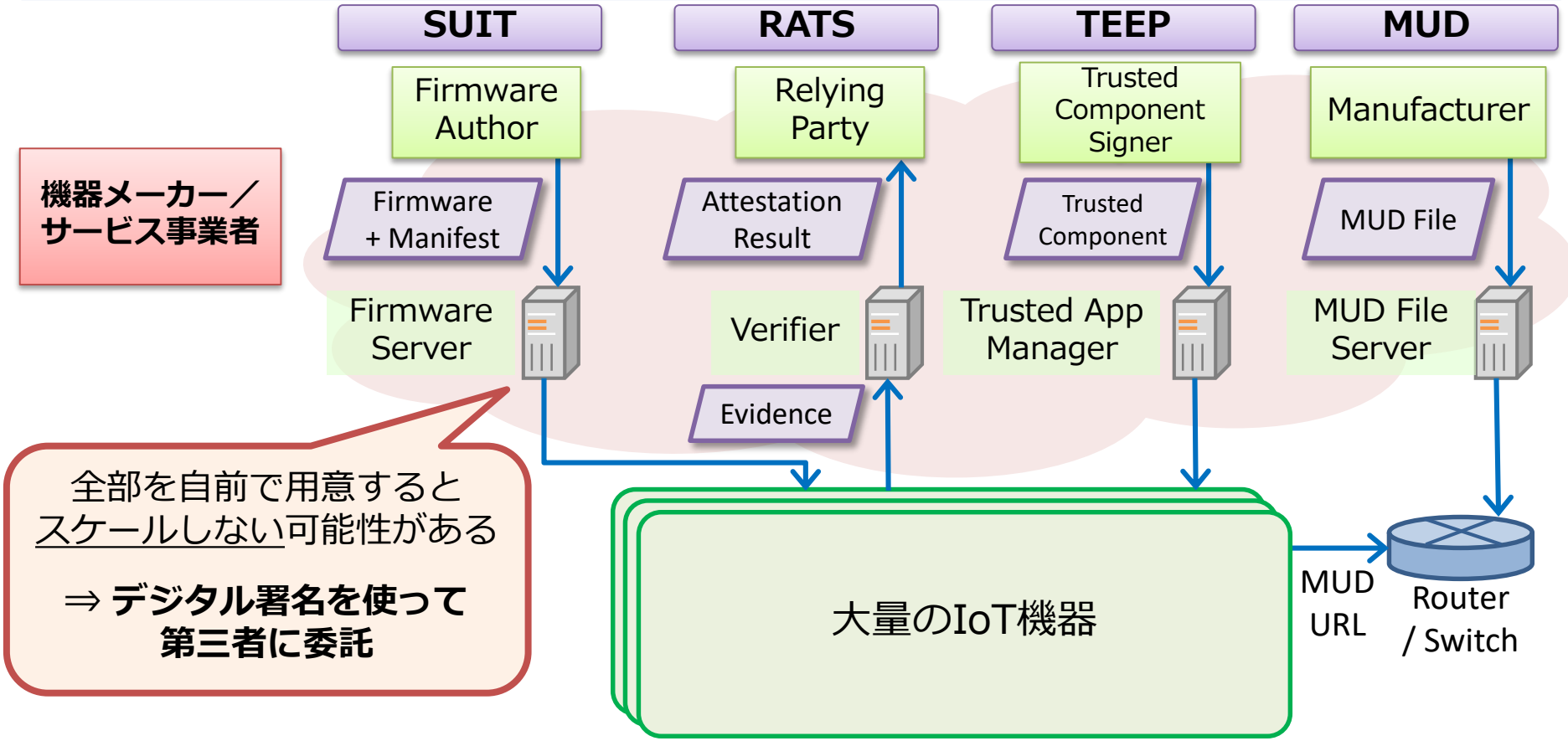
IoTの課題 － 遠隔での機器管理 －

信頼される安心を、社会へ。
SECOM



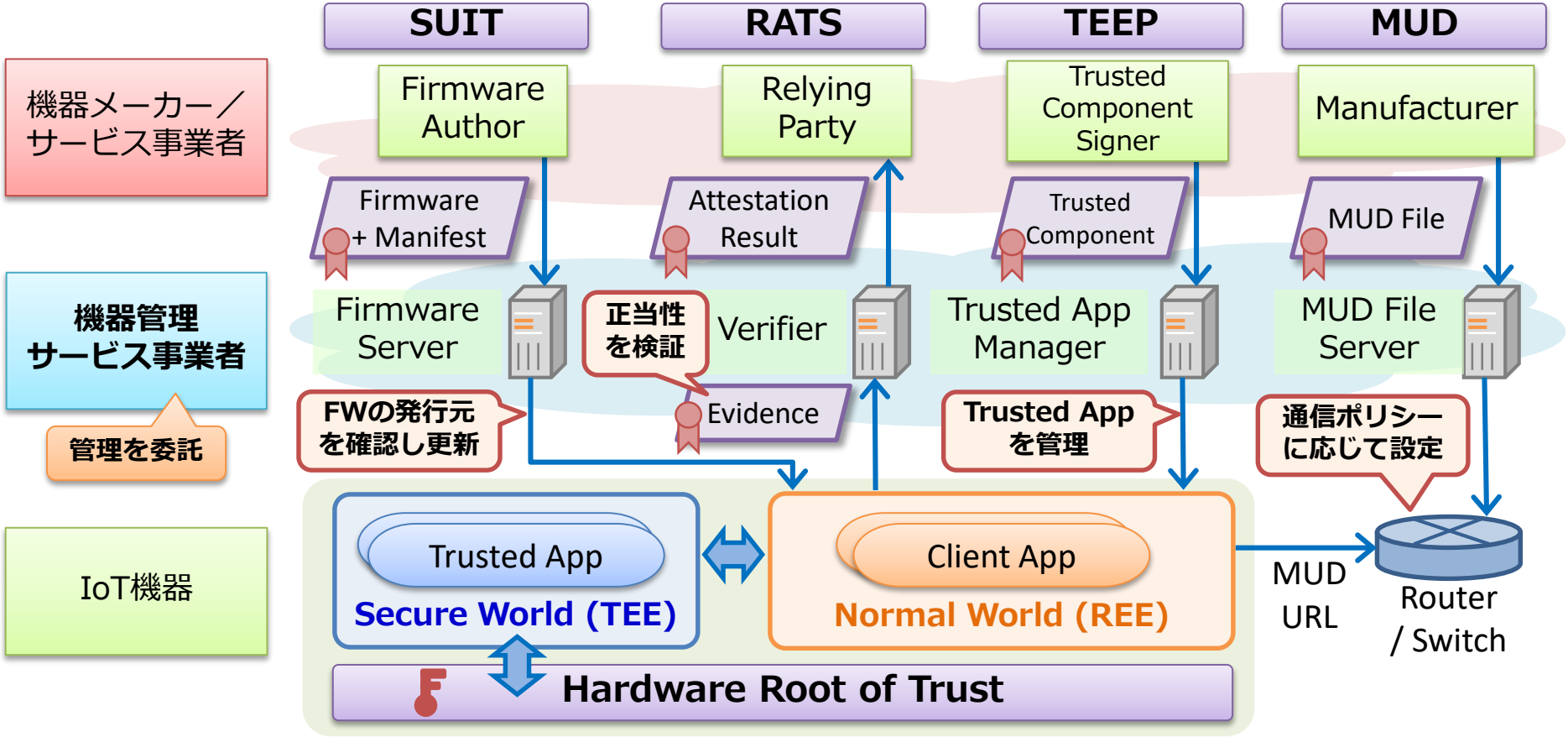
周囲の環境が変わっても、IoT機器を遠隔から安全に管理したい

機器管理技術の標準化の意義 - スケールの視点 -



IoT機器管理技術の標準化 - 全体像 -

信頼される安心を、社会へ。
SECOM



SUITの動向 - IoT機器の安全なファームウェア更新 -

信頼される安心を、社会へ。
SECOM

- **WG Draftの動向**
  - アーキテクチャ（draft-ietf-suit-architecture-14）と
    情報モデル（draft-ietf-suit-information-model-08）がIESGにおいてレビュー中
- **Secure Reporting of Update Status**
  - draft-moran-suit-report-00
  - ファームウェア更新結果（失敗理由など）を報告するフォーマット（SUIT Report）を定義
  - ユースケースとしてTEEPが想定

SUIT + MUD (IoT機器の安全なネットワーク接続)

- **Strong Assertions of IoT Network Access Requirements**
  - draft-moran-suit-mud-01
  - MUDファイルをSUITの方式でダウンロードするために、SUIT Manifestの拡張を定義
  - WG Draftとして採用するかどうかは議論を継続

TEEPの動向 - 機密性の高いアプリの遠隔管理 -

信頼される安心を、社会へ。
SECOM

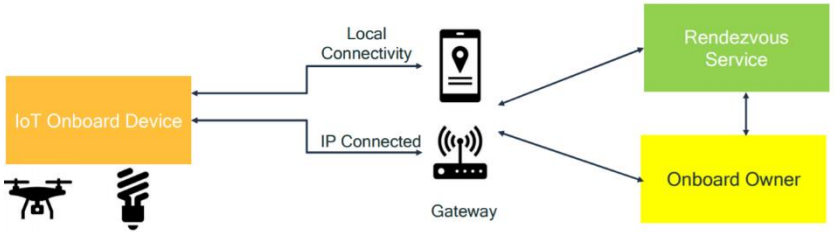
- **WG Draftの動向**
  - draft-ietf-teep-architecture-13 ：用語定義の修正や応用範囲の追加テキストについて議論
  - draft-ietf-teep-protocol-04 ：SUITやRATSに対する依存部分について議論
- **Hackathon**
  - TAM Server
    - ✓ Dave (Microsoft) : https://github.com/dthaler/OTrP
    - ✓ Isobe (SECOM) : https://github.com/ko-isobe/tamproto
  - TEEP Agent
    - ✓ Tsukamoto (AIST), Nagata, Kikuchi (Lepidum) ：TEEP-Device
    - ✓ Takayama (SECOM) : https://github.com/yuichitk/libteep
    - ✓ Dave (Microsoft) : https://github.com/dthaler/OTrP

IETF108 Hackathonで瀧田が実装／公開したOSSを更新

TEEP Hackathonでは、日本から積極的に参加があった

RATSの動向 - IoT機器の正当性の検証 -

- **WG Draftの動向**
  - draft-ietf-rats-architecture-07 ：
    - ✓ WGLCにむけてレビューが進行中
  - draft-ietf-rats-eat-04 ：
    - ✓ Attestation ResultsへのEAT利用や、TEEなどにおける実行状態のMeasurementを議論
- **FIDO and EAT dependencies**
  - EATドラフトの共著者の方がFIDOの動向を発表
  - IoTのオンボーディングプロトコルを標準化中
    - ✓ FIDO IoT spec, Working Draft, Aug/2020
  - リクエスト
    - ✓ EATはまだ標準化されておらず、EATが提案するClaimはIANAに未登録
    - ✓ FIDOが期待する最小のClaims（Nonce, UEID）を早く登録してほしい
    - ✓ FIDOにおける標準化が完了しないため



出典：https://datatracker.ietf.org/meeting/109/materials/slides-109-rats-sessb-fido-updates-to-rats-00

IoT Operations WG (IOTOPS) の提案 @ IETF 109

- **Area** ：Operations and Management Area (ops)
- **チェア**：Alexey Melnikov, Henk Birkholz
- **経　緯**：去年から複数のSDOを跨ぐ議論の場が要望されていた
- **目　的**：

① IoT機器のオンボーディングとライフサイクル管理に関する運用上の問題を議論

- ✓ 出荷時のプロビジョニング、EOL (End Of Life) 管理
- ✓ NWリソースに対するIoT機器のアクセス制御、隔離／検疫
- ✓ ソフトウェア／ファームウェアのアップデート

② IoT機器の運用に関するセキュリティの課題を議論

③ 運用面の実践と要求事項を文章化して発行

- 外部から新しい議論をIETFに持ち込む場合、妥当なWGにディスパッチする

まとめ　- データモデルと機器管理技術の標準化動向 -

信頼される安心を、社会へ。 SECOM

① IoTデータモデルの標準化動向

- ASDF： SDO間で相互変換可能なデータモデルフォーマット(SDF)の策定

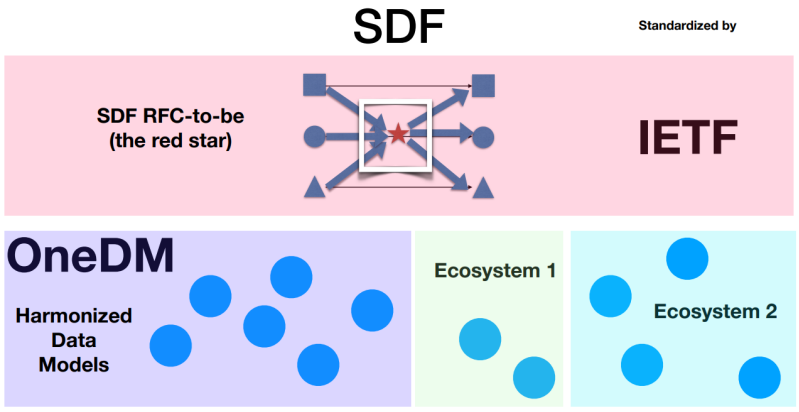
② IoT機器管理技術の標準化動向

- SUIT： MUDをサポートするI-Dの提案
- TEEP： SUITやRATSへの依存部分の議論
- RATS： Claimsに関するFIDOからの要求

③ 今後の動向

- IoT Operations WGの提案

WGやSDOを跨ぐIoTデータモデル／
セキュリティの議論が活発になっている！



出典：https://www.ietf.org/proceedings/108/slides/slides-108-asdf-consolidated-slides-02