信頼される安心を、社会へ。
SECOM

JNSA標準化部会ビギナーズセミナー
IoTセキュリティ標準化の動向を知る

IoTセキュリティとIETF標準化

セコム IS研究所 /
セキュアオープンアーキテクチャ・エッジ基盤技術研究組合
磯部 光平
ko-isobe@secom.co.jp

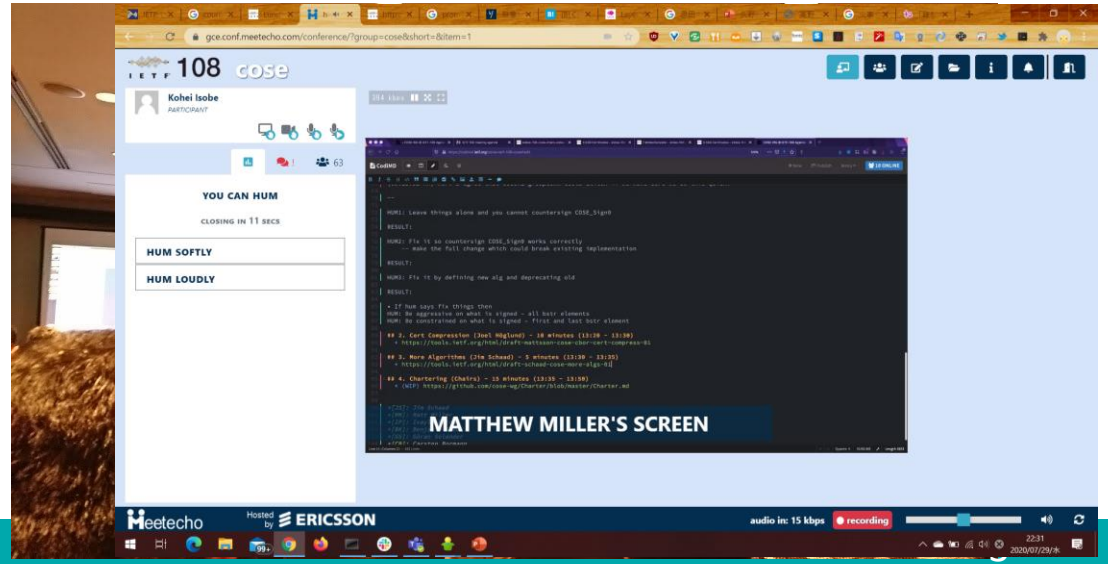
自己紹介

- 磯部 光平
  (いそべ こうへい)
- 略歴
  - 2016年 セコム入社 IS研究所
    コミュニケーションプラットフォームDiv. 暗号・認証基盤グループ
  - 2020年 セキュアオープンアーキテクチャ・エッジ基盤技術研究組合(TRASIO) 兼務
    IoT向けエッジセキュリティ研究に従事
  - 2022年 セコムIS研究所 デジタルプラットフォームDiv. サイバーフィジカルセキュリティG
- 研究領域
  - 暗号システム、デバイス管理システム、PKI

IETF (Internet Engineering Task Force)

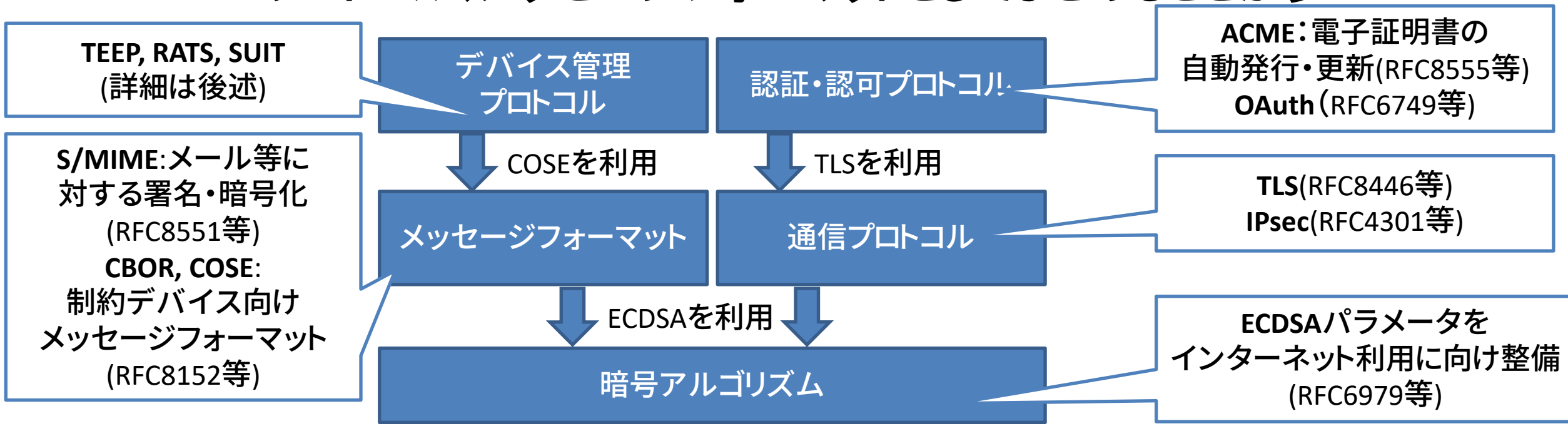
信頼される安心を、社会へ。
SECOM

- インターネットをよりよく機能させるため、
  良質な技術文書の作成が使命
- フォーラム標準
  - 標準化文書はRFC(Request for Comments)として発刊
- 標準化プロセス
  - 誰でも参加可能。会員制度はなく
    個人として参加
  - 主にメーリングリストで議論
  - F2F会議を年3回開催。
    昨今はハイブリッド化



セキュリティに関するIETFの取組

- secエリア
  - IETFの6つの技術領域のうちの一つ
  - セキュリティ関連技術を幅広く取り扱う
    - プロトコル、メッセージフォーマットとしてまとめることが多い



IETF標準のモットー

- *An unofficial motto of the IETF is,*
  "We believe in rough consensus and running code."
  - 実運用性を重視する
  - 実装に基づくフィードバックが歓迎される

標準化文書の議論

文書・仕様案

実装を経た知見
フィードバック

会議直前の土日に開催

実装A

実装B

実装・ハッカソン

IETF Hackathon

信頼される安心を、社会へ。
SECOM

- Meeting直前の土日に開催
- IETFに関連するテーマ・有志で活動可能な場
  - 作業場、食事などが提供される
  - 標準仕様のディスカッション、実装、プラグテストなど活動は多種多様
  - Hackathon成果は、仕様案の修正やMeetingの議題につながる

IoTに関連したIETFの取り組み

- Constrained Device (制約付きデバイス,RFC7228)
  - 処理性能や消費電力に制約のあるデバイスという位置づけ
  - Classが定義され、ターゲットデバイスの指定などに使われる

Name	data size (e.g., RAM)	code size (e.g., Flash)
Class 0, C0	<< 10 KiB	<< 100 KiB
Class 1, C1	~ 10 KiB	~ 100 KiB
Class 2, C2	~ 50 KiB	~ 250 KiB

Table 1: Classes of Constrained Devices (KiB = 1024 bytes)

- IoTデバイス向け規格
  - CoAP(Constrained Application Protocol)
    HTTPレイヤーに相当する通信プロトコル
  - ACE(Authentication and Authorization for Constrained Environments)
    IoTデバイスでも動作可能なの認証プロトコル

IoTセキュリティ技術を取り巻く状況

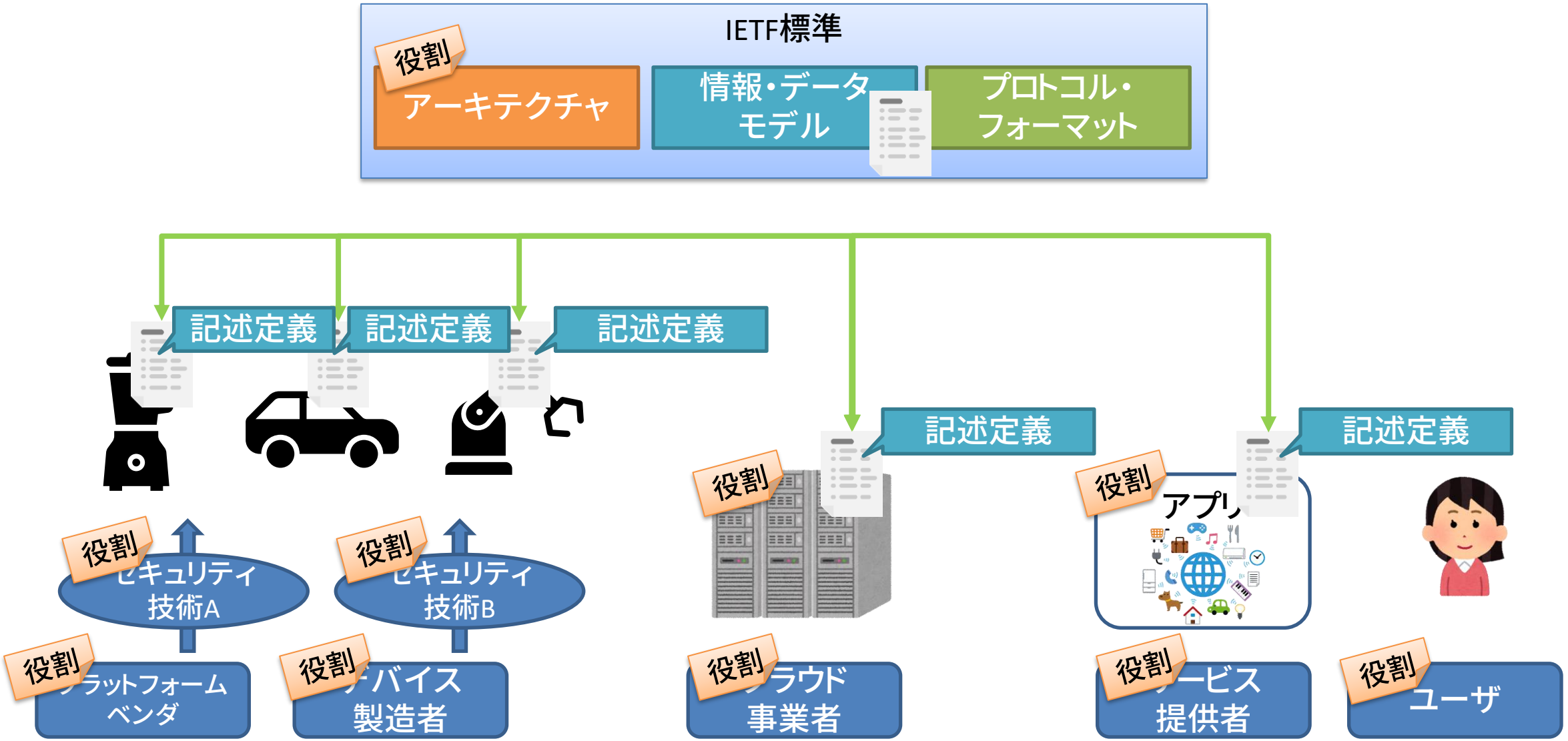
信頼される安心を、社会へ。
SECOM

- セキュリティ技術：プロプライエタリ実装が多い
  - TEE：ARM TrustZone, Intel SGX, …
  - セキュアブート・アテステーション：商用製品への実装例
  - 実装はハードウェアや特定プラットフォームに依存する傾向があり、広範なセキュリティ技術の標準は不在

- IETF標準の果たす役割
  - セキュリティ技術の整理
    - 複数のプラットフォームで共通して活用できる
  - インターネット上での運用や管理に資する
    - 製品開発のみならず運用上も安全性や効率性を確保する

IETFの考え方(私見)

- 出発点
  - エンジニアリング視点から、具体的な脅威への対抗や利用可能なセキュリティ技術の活用を図る
  - インターネット標準の存在が相互運用性の向上など利益をもたらす
- 何を標準とするか
  - アーキテクチャ
  - 情報モデル・データモデル
  - プロトコルやフォーマット
- 具体的な機能仕様を決めて、強制化するわけではない
  - RFC(Request for Comments)
  - 仕様をどう使うかは、実装者や設計者次第
    - 実装・設計者にとって使いやすい標準であることが求められる

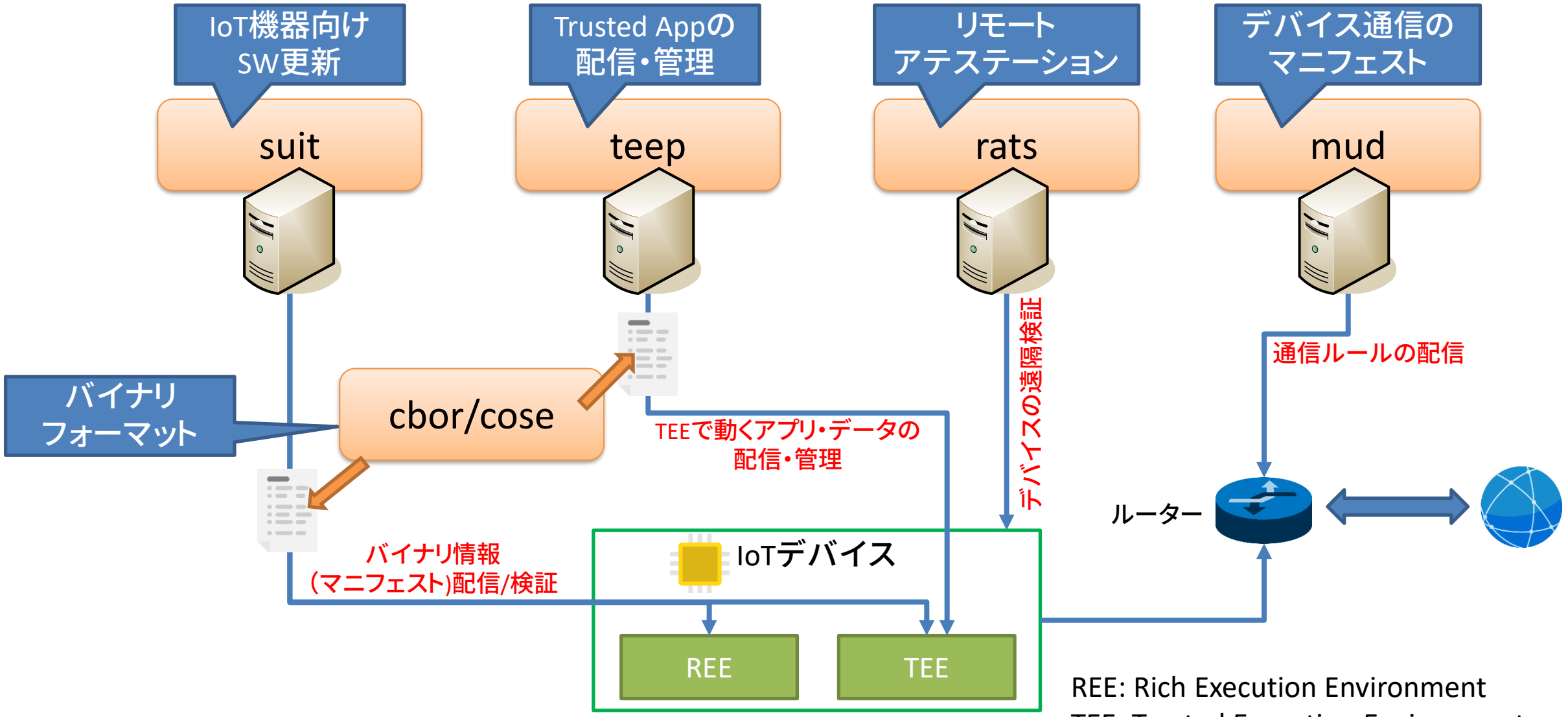


デバイス管理に関わるIETF標準

信頼される安心を、社会へ。
SECOM

- teep Trusted Execution Environment Provisioning
  - TEE上で動くアプリ・データを遠隔配信する
- suit Software Updates for IoT
  - ソフトウェア更新用マニフェストを生成・処理する
- rats Remote ATtestation procedureS
  - リモートアテステーション(遠隔検証)用データの生成と検証
- これら標準は相互に依存関係や共通項目を持つ
  - teep: ratsで配信先デバイスを検証し、suitマニフェストを配信する
  - いずれの規格も制約付きデバイス用に同一のバイナリフォーマット(cbor/cose)をサポート

デバイス管理に関連するプロトコル



REE: Rich Execution Environment
TEE: Trusted Execution Environment

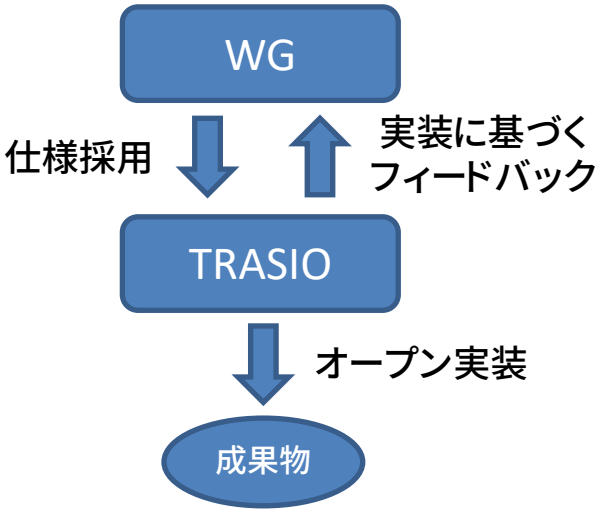
IETF標準化活動への参加事例

信頼される安心を、社会へ。SECOM

Trusted Appの配信・管理

teep

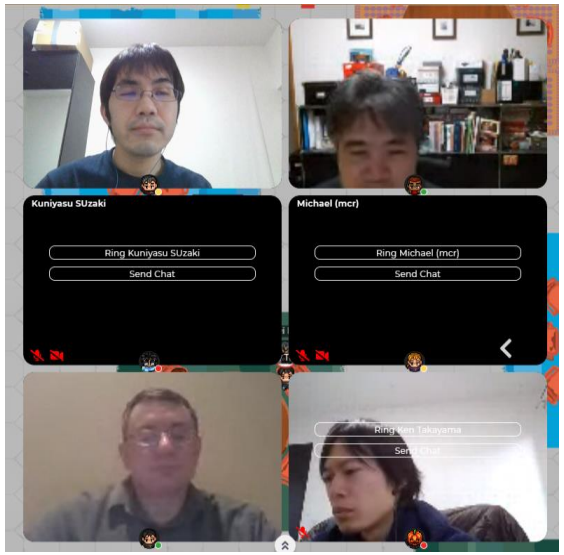
- プロジェクトメンバーが議論やハッカソンに参加。RFC共著
- ドラフト仕様の実装ならびに公開
  tamproto https://github.com/ko-isobe/tamproto
  teep-device
- 実装に基づくフィードバック



IoT機器向けSW更新

suit

- Teepにおけるバイナリイメージ配信用途に採用
  →teepでの使用時の仕様検討やフィードバックを実施
- ライブラリのOSS公開
  libcsuit https://github.com/yuichitk/libcsuit



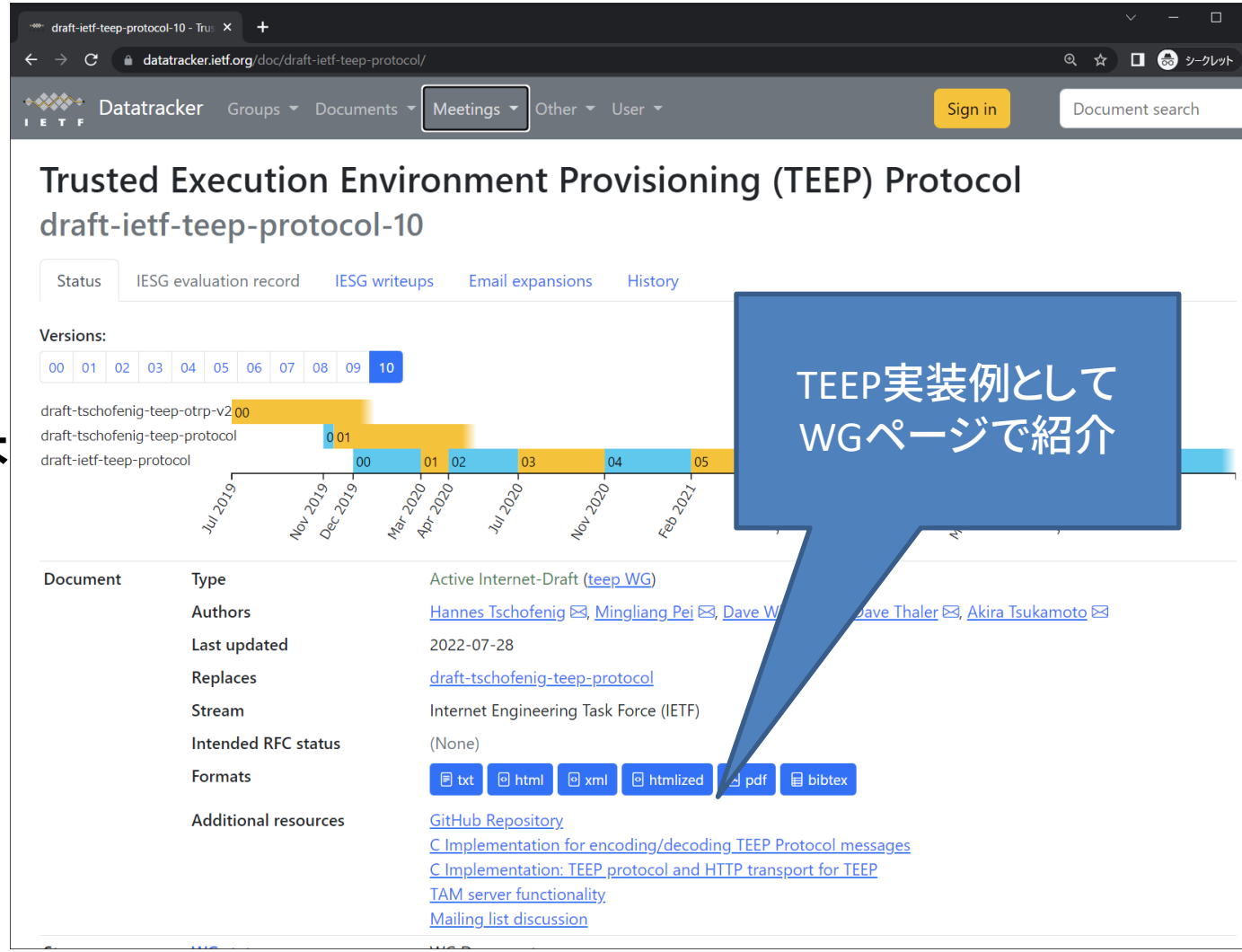
リモートアテステーション

rats

- アテステーション仕様として採用
- 現在、TEEP用のプロファイル策定や実装評価が進行中

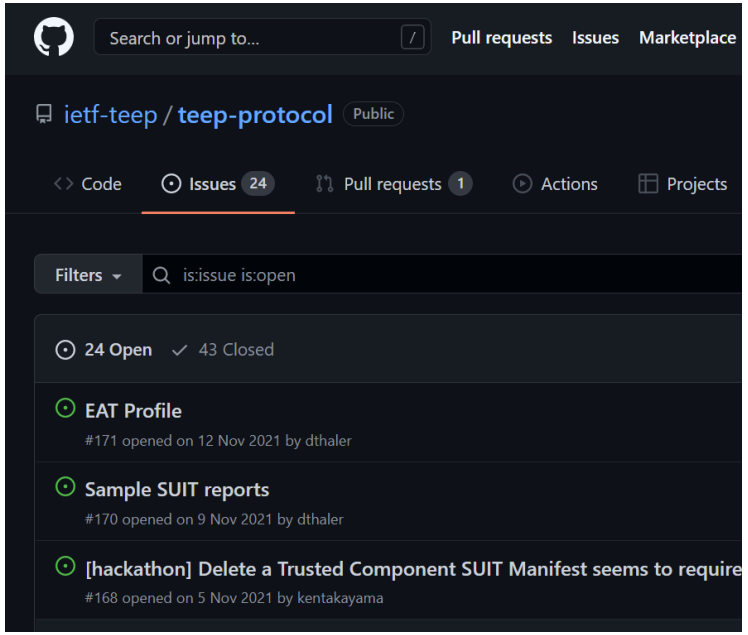
WGの貢献

- WGへの影響
  - 実装視点からのフィードバックを中心に貢献
    - IoTデバイスへの適用可否
  - WG主要メンバーとして仕様策定をリード



IETF活動をウォッチするには

- Datatracker https://datatracker.ietf.org/wg/#sec
  - 作成中のドラフト、ミーティング議事録、メーリングリストへのリンクなどが集約
- IETF meeting
  - 会議は事後にYoutubeで公開
  - ISOC-JPなど国内向け報告会
- GitHub
  - ドラフト作成の実作業場。



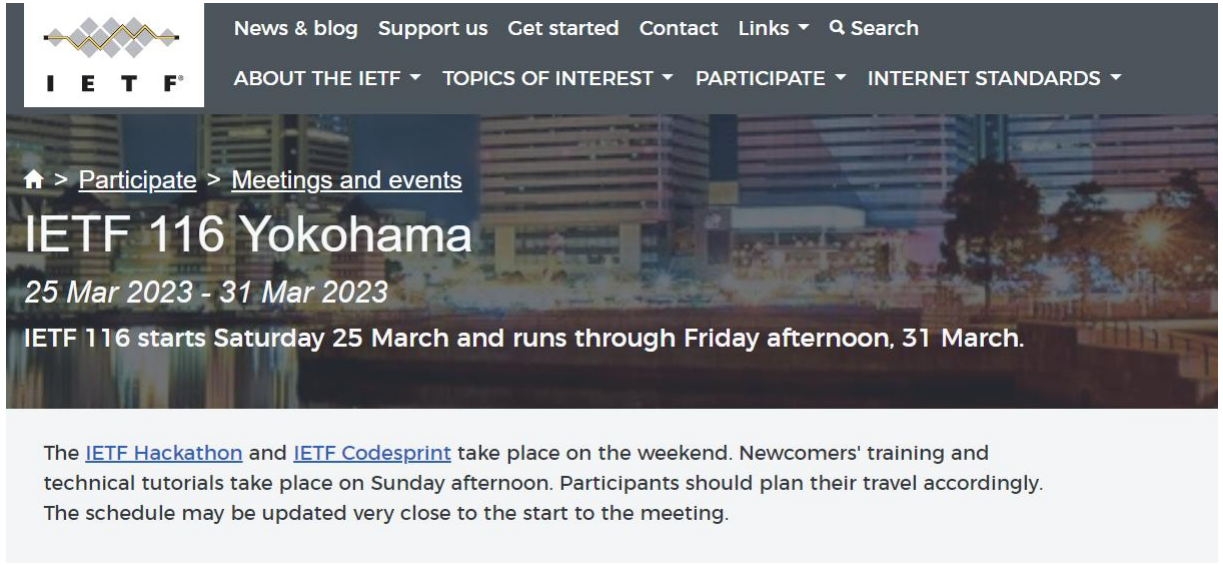
IoTセキュリティにおけるIETF標準化の傾向

信頼される安心を、社会へ。
SECOM

- ボトムアップな提案
  - エンジニアリング視点から、具体的な脅威や利用可能なセキュリティ技術を背景に持つ標準化提案がなされる
  - 既存実装を収容できる相互運用性の確保
- 価値基準
  - セキュリティ・プライバシーの観点において、ユーザ保護を第一とする
    - IoTシステムの直接の所有者と言えるデバイスベンダやサービス提供者よりもしばしば優先される
  - 概念的な標準よりも実装可能・利用可能な文書をゴールとする
  - インターネット全体の改善に資するか
    - 特定のドメインのみの問題解決は受け入れられにくい
- 標準化プロセス
  - 各参加者は個人として扱われる。
    - 相互運用性の観点から、必要に応じて他のSDOとのリエゾンは随時行う
  - 良質な標準でなければ使われないというインセンティブが存在。
    - RFCは標準であるものの、強制力はない。

IETF116 Yokohama

- 7年ぶりの日本開催
- 2022年3月27日～3月31日
  - ハッカソン：25日(土) 26日(日)
  - ハッカソンは無料



https://www.ietf.org/how/meetings/116/

まとめ

- IETF標準化
  - 標準化プロセスの特徴、secエリア
- IoTとIETF
  - IoTの整理
    - Constrained Device
  - IoTセキュリティ分野の標準化
    - ハードウェアベースのセキュリティ技術の活用
    - デバイスマネジメントに係るプロトコル
SUIT, TEEP, RATS
- 標準化活動の事例
  - 実装に基づくフィードバック
  - IETF Hackathon
  - ウォッチ・参加方法