

ISOC-JP IETF114報告会

IETF114参加報告 - COVID-19, IoT関連 -

セコム IS研究所
磯部 光平, 高山 献

{ko-isobe, takayama-ke}@secom.co.jp

自己紹介

信頼される安心を、社会へ。

SECOM

- 磯部 光平
- 略歴
 - 2016年 セコム 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G.
 - 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) 研究員
IoT向けエッジセキュリティ研究に従事
- 研究領域
 - 暗号利用システム、デバイス管理システム、PKI



当地(米国)の状況

- CDCによる公共交通機関におけるマスク着用令は2022年4月に失効
 - Mask is required.というアナウンスは見られるが、旅客のマスク着用者は少数



IETF114でのCOVID-19対策

信頼される安心を、社会へ。

SECOM

- ・ ルール
 - 原則マスク着用。発言時のみマスク取り外し可
 - WG開始時にChairが上記アウンス
 - 参加者は大半が協力し、マスク着用者が多かった
 - ワクチン接種推奨(ただし接種証明は求めない)

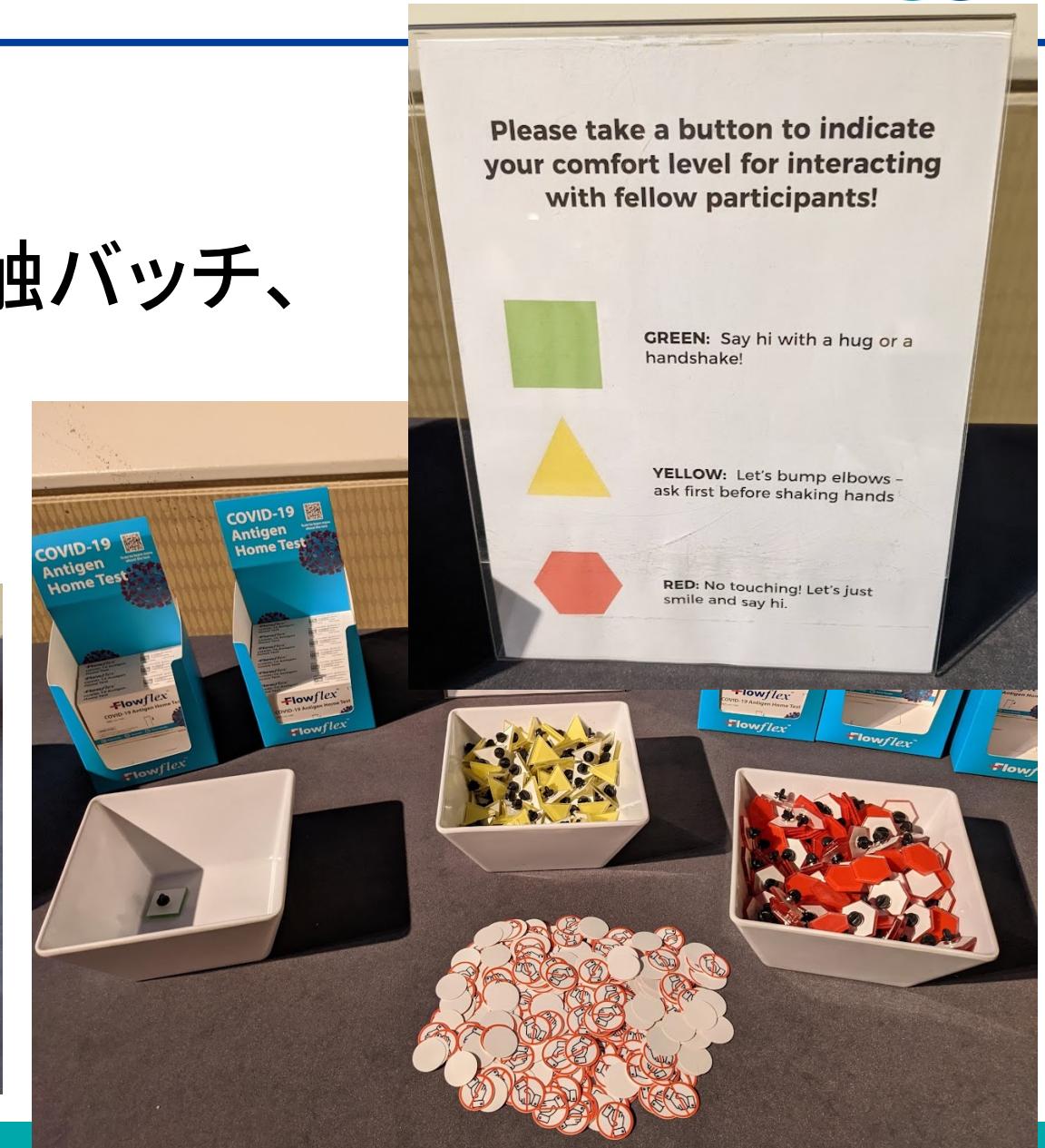
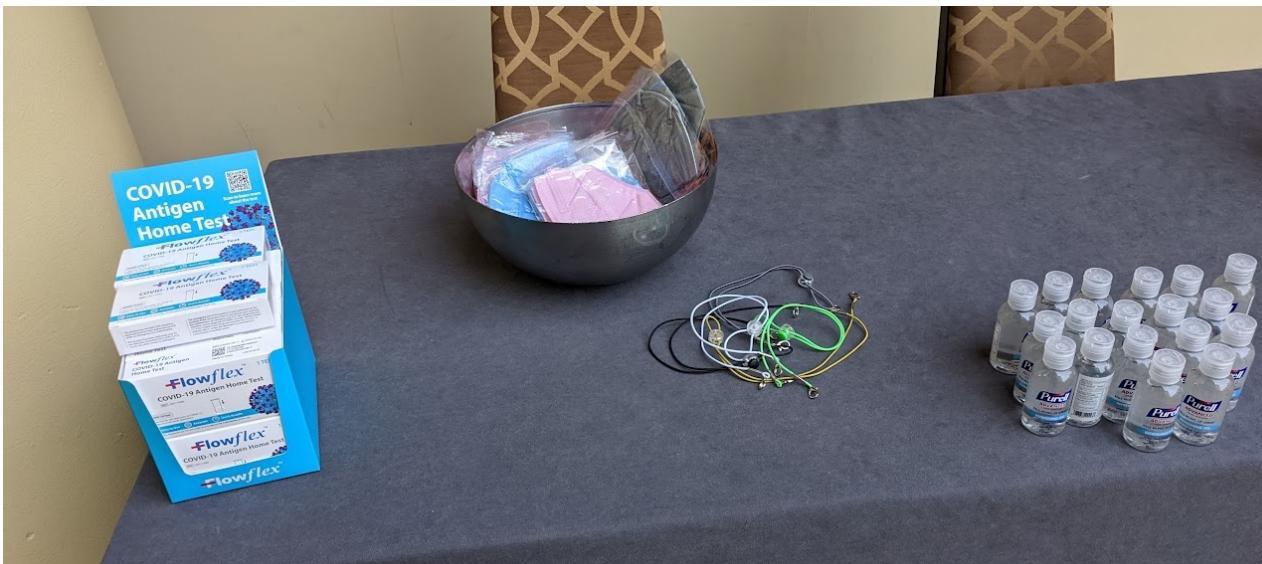


IETF114でのCOVID-19対策

信頼される安心を、社会へ。

SECOM

- 資材
 - マスク、抗原検査キット、接触バッヂ、除菌ジェル

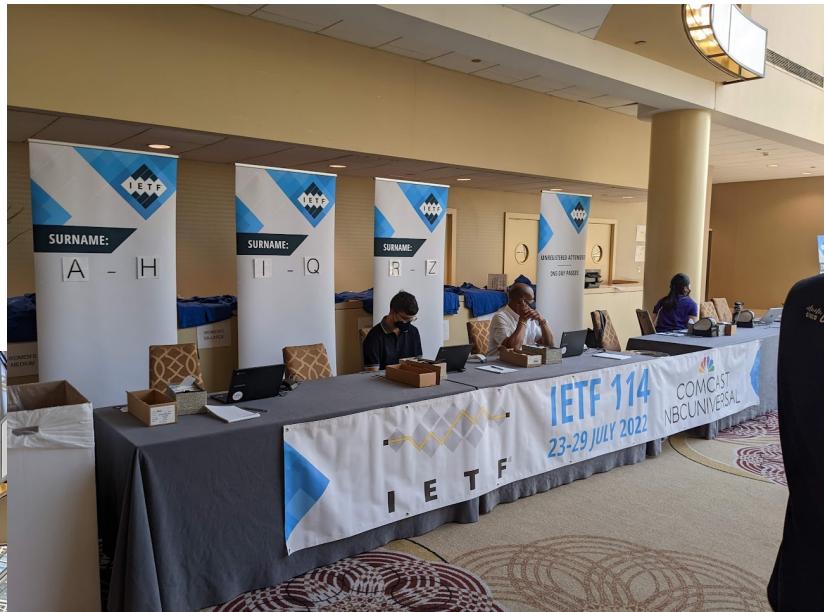


IETF114でのCOVID-19対策

信頼される安心を、社会へ。

SECOM

- 会場サービス
 - スナックなどは通常通り



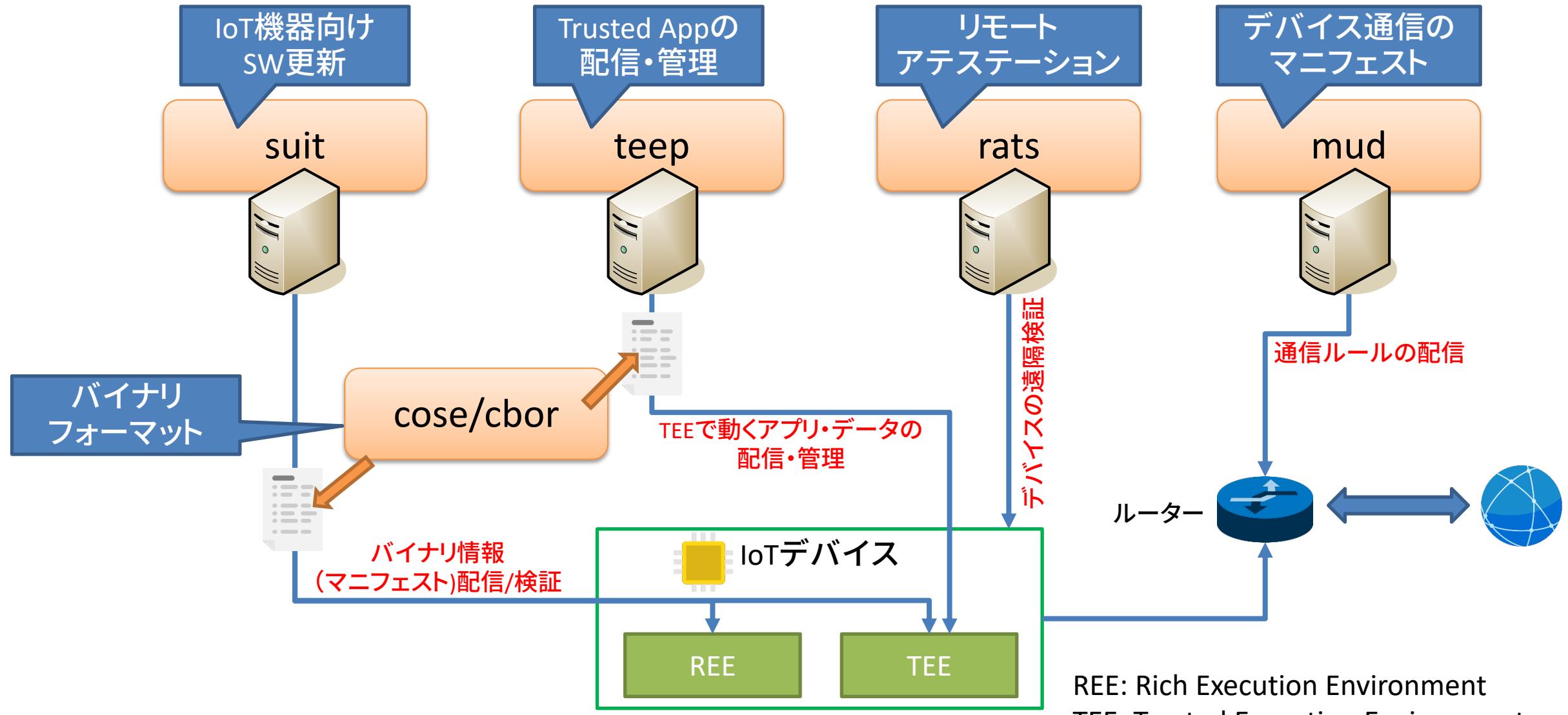
- For IETF 113 Vienna we had 9 reported cases from 314 onsite participants (2.9%)
- For IETF 114 Philadelphia we had **16 reported** cases and 2 people who were ill but tested negative, from 622 onsite participants (**2.6% at 16**, 2.9% at 18)

- IETFのCOVID-19対策

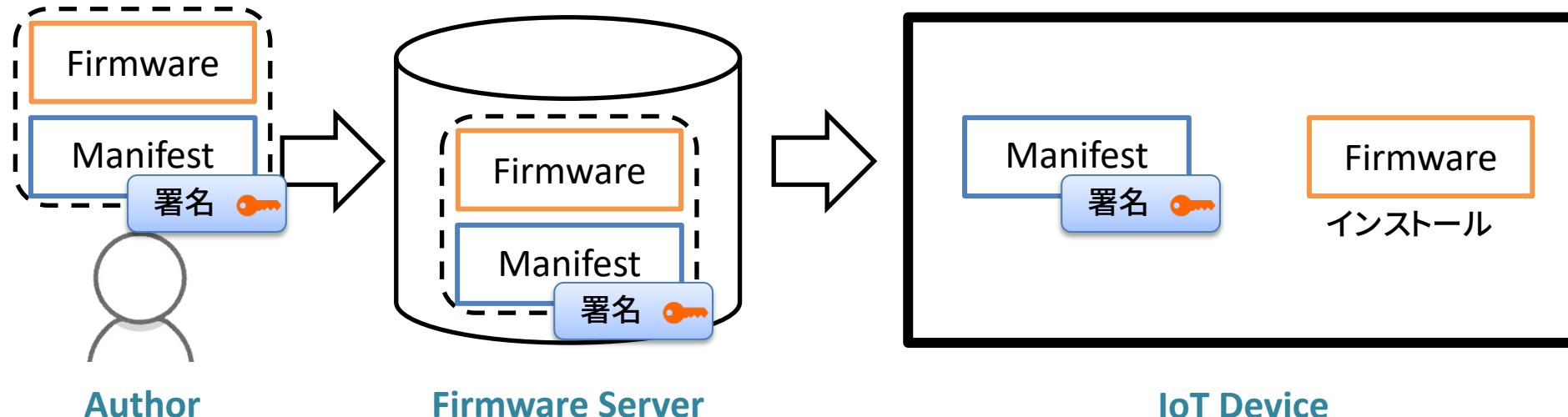
- 当地の水準からすれば高い水準の基準を課している。
- 参加者も協力的。
- 参加者数は回復傾向にあり、会議のありかたは議論継続中

IOT関連

デバイス管理に関するプロトコル

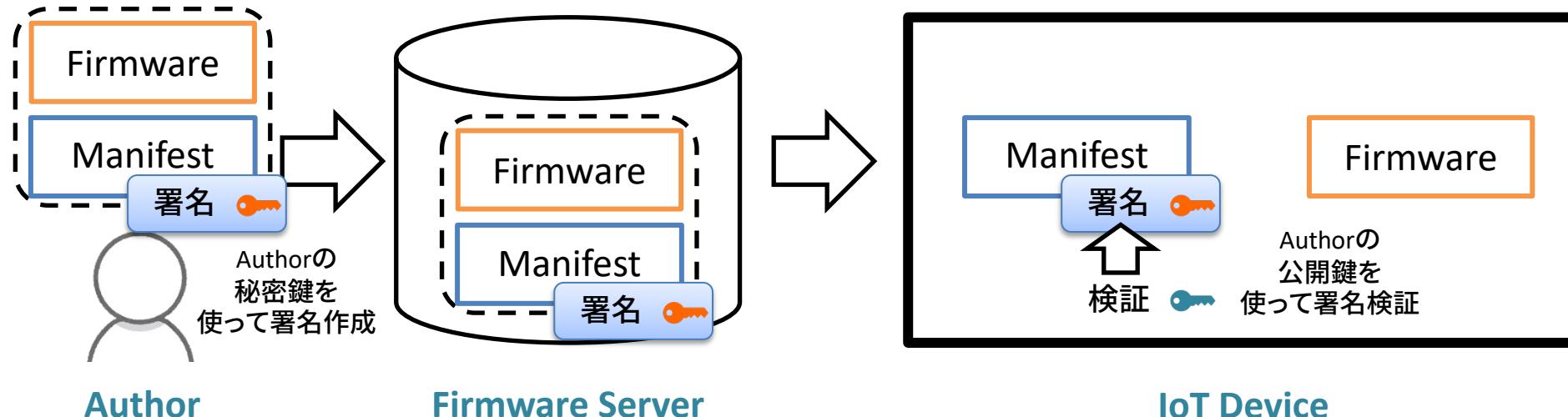


- 目的: IoT機器のFirmwareの更新を行う
 - Firmwareの更新を安全に実行できる
 - 制約の強い機器(e.g. 10~100KB RAM)でも動作する
- SUIT Manifest
 - Firmwareの取得・検証・インストール手順を記述する



SUIT Working Group

- 目的: IoT機器のFirmwareの更新を行う
 - Firmwareの更新を安全に実行できる
 - 制約の強い機器(e.g. 10~100KB RAM)でも動作する
- SUIT Manifest
 - Firmwareの取得・検証・インストール手順を記述する
 - Authorによって電子署名が付けられ、配送途中で改ざんされてもDeviceは署名検証することで検知できる



SUIT Working Groupの進捗

- SUIT Architecture
 - SUITに登場する各者の役割を明確にする
 - [RFC9019](#)になった(2021/04)
- SUIT Manifest ([draft-ietf-suit-manifest](#))
 - SUIT Manifestのデータ形式を標準化する
 - v18が出た(2022/07)
 - Working Group内で同意を取っている(Last Call)最中
- SUIT Firmware Encryption ([draft-ietf-suit-firmware-encryption](#))
 - 暗号化したFirmwareを配達する際のManifestを標準化する
 - v06が出た(2022/07)
 - まだまだ適切なデータ形式を模索中

- TEE：セキュアな隔離実行環境
 - TEE内の平文データにはREE内から直接読み書きできない
 - 指紋などの生体情報を安全に管理できる
 - 改変されていない指紋認証プログラムを実行できる
 - スマートフォンを中心に利用が広がっている
 - 現在はスマートフォンベンダーが占有して管理している
 - クラウドを含めTEE内で動かすアプリが増えていく（予想）



REE: Rich Execution Environment

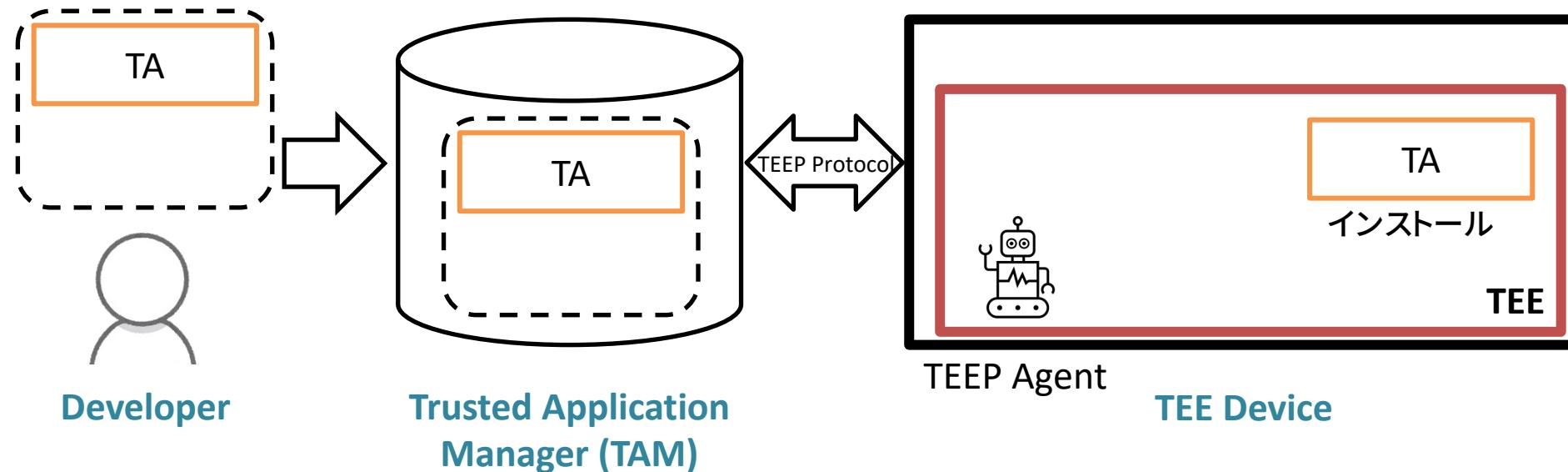
TEE: Trusted Execution Environment

TEEP Working Group

信頼される安心を、社会へ。

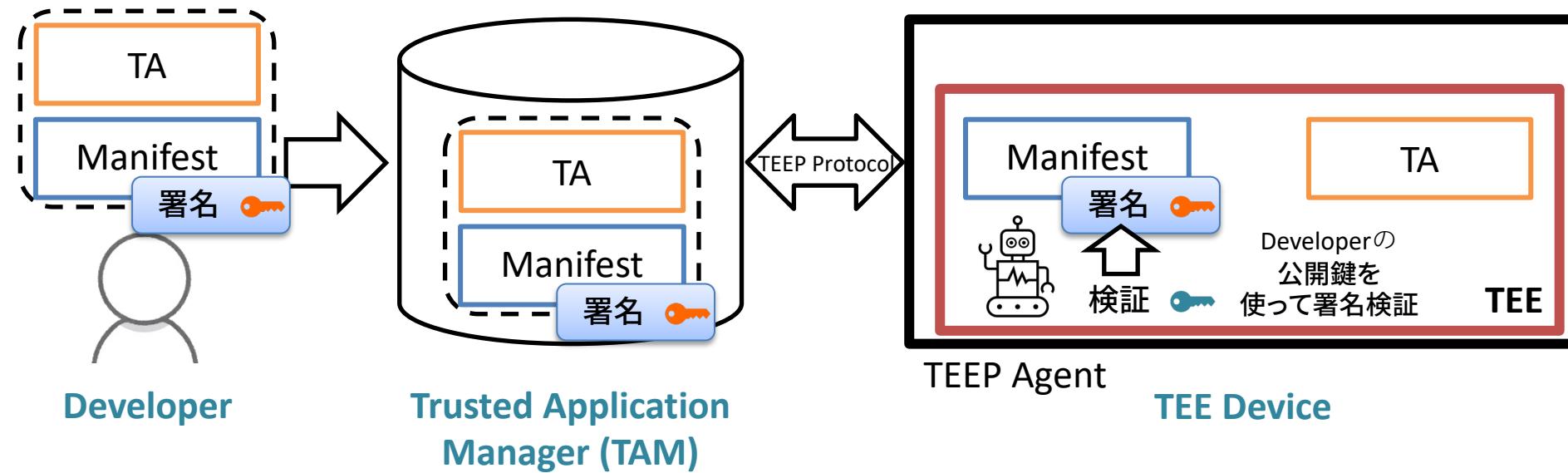
SECOM

- 目的：安全なTEE用アプリ・コンフィグの配信
 - Developerが作ったTrusted Application (TA)を
 - Trusted Application Manager (TAM)が配信し
 - TEEを搭載したデバイスにインストールする



TEEP Working Group

- TEEP Protocol : 安全にTAの配信をするプロトコル
 - AgentとTAMは認証しあう→なりすまし・改ざんを防ぐ
 - TEE Deviceごとに適切なTA・コンフィグを配信する
 - TEEのインストール手順はSUIT Manifestで記述する



TEEP Working Groupの進捗

信頼される安心を、社会へ。



- TEEP Architecture ([draft-ietf-teep-architecture](#))
 - TEEPに登場する各者の役割を明確にする
 - v18 (2022/07)、RFCにするために最終調整中
- TEEP Protocol ([draft-ietf-teep-protocol](#))
 - TEEP Protocolのメッセージ形式を標準化する
 - v10が出た (2022/07/28←IETFミーティングの最中)
- TEEP over HTTP ([draft-ietf-teep-otrp-over-http](#))
 - TEEP ProtocolのメッセージをHTTP上で送信する
 - v13 (2022/02)、RFCにするための最終調整中

ハッカソンの様子

- TEEP WG、SUIT WG、COSE WGの合同で開催

AIST
TEEP 塚本さん、高山、Daveさん
Microsoft



Arm
SUIT 高山、Hannesさん



SECOM
TEEP 磯部さん、Daveさん



Qualcomm
COSE Laurenceさん、Davidさん、Hannesさん
Linaro



- **TEEP WG**

-  使用する署名方式の合意方法の議論 (Dave、磯部、高山)
-  TEE Deviceの情報取得データ形式の議論 (Dave、磯部、塚本)
-  COSEのデータフォーマット記述言語の検証 (塚本)

- **SUIT WG**

-  Firmwareを暗号化したときのSUIT Manifest検討
 - ドキュメントを作成 (Hannes)
 - 適切なSUIT Manifestを試作・ドキュメントの改善提案 (高山)

- **COSE WG**

-  署名以外に、暗号化・MACにも対応 (Laurence、David、Hannes)
 - ドキュメント自体はあるがt_coseというライブラリには未実装

実装を公開しています

- TEEP
 - tamproto: <https://github.com/ko-isobe/tamproto>
 - libteep: <https://github.com/yuichitk/libteep>
- SUIT
 - libcsuit: <https://github.com/yuichitk/libcsuit>