信頼される安心を、社会へ。
SECOM

IoT機器のセキュリティに関する IETFの標準化動向

― Lifecycle of Things ―

2020年7月6日

セコム株式会社　IS研究所
瀧田悠一

本活動の一部は、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。
2019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」
http://www.ttc.or.jp/j/info/topics/20190411/

©2020 SECOM CO., LTD.　本発表専用の資料となりますので第三者への開示・転用はお控えください。

自己紹介

信頼される安心を、社会へ。
SECOM

【名前】

瀧田 悠一（たきた　ゆういち）

【所属】

セコム株式会社　IS研究所

【略歴】

- **入社後**：　監視カメラシステムの開発
- **現在**：　IoTプラットフォームの研究開発
- **IETF**：　IoTセキュリティに関する技術を主に調査
  IETF 103からHackathonを含めて継続的に参加

©2020 SECOM CO., LTD.　本発表専用の資料となりますので第三者への開示・転用はお控えください。

目次

- IoT機器のライフサイクル管理、課題と解決策
- IETFでの国際標準化の動向
- 今後の展望

©2020 SECOM CO., LTD.
本発表専用の資料となりますので第三者への開示・転用はお控えください。

IoTサービスの事例　― セコムのオンラインセキュリティ ―

信頼される安心を、社会へ。 SECOM

- IoT機器を用いて、1秒でも早く、異常を見つけ・状況を把握し・対処する

- **サブスクリプション型**のビジネスモデル
- **約6000万個**のセンサーを活用

IoT化の進展 ― クラウドと連携する監視カメラ ―

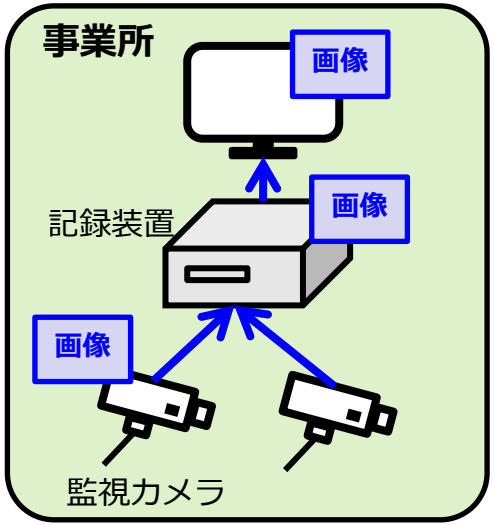
信頼される安心を、社会へ。
SECOM

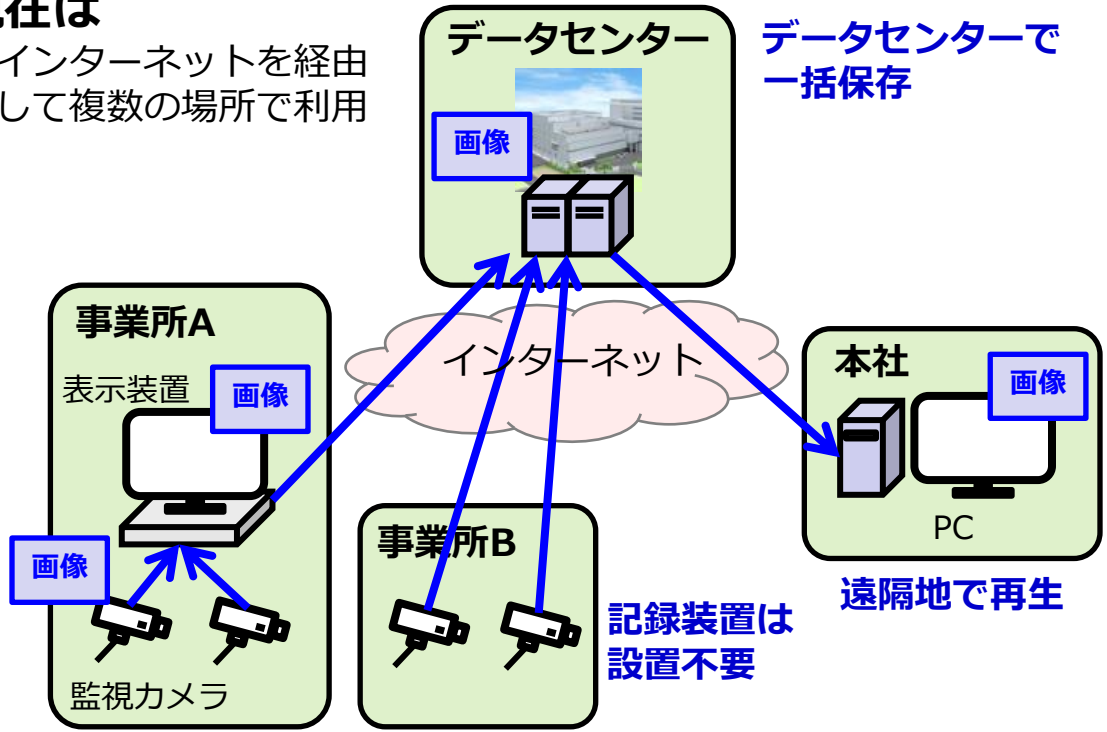
以前は

・クローズドな環境で運用
・CCTV(Closed Circuit TeleVision)

現在は

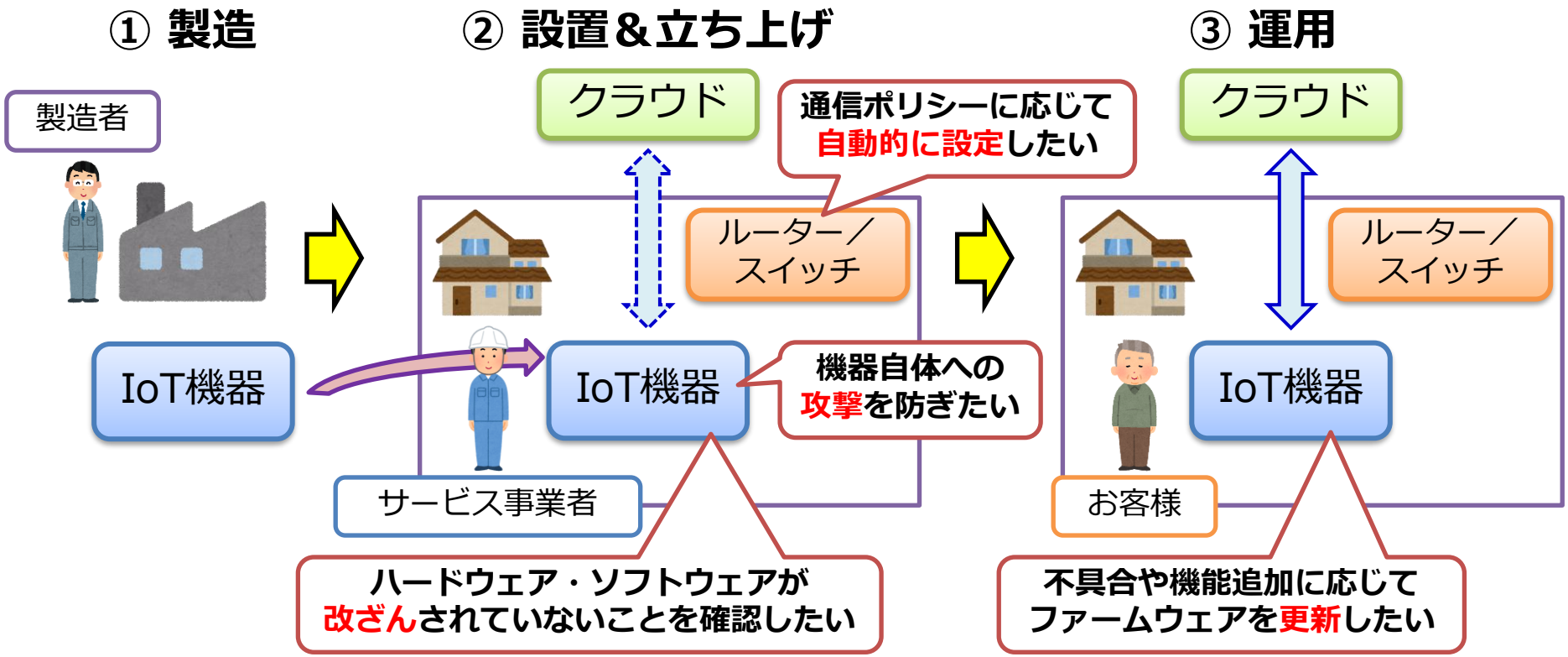
・インターネットを経由して複数の場所で利用





機器を遠隔から管理する仕組みが必要

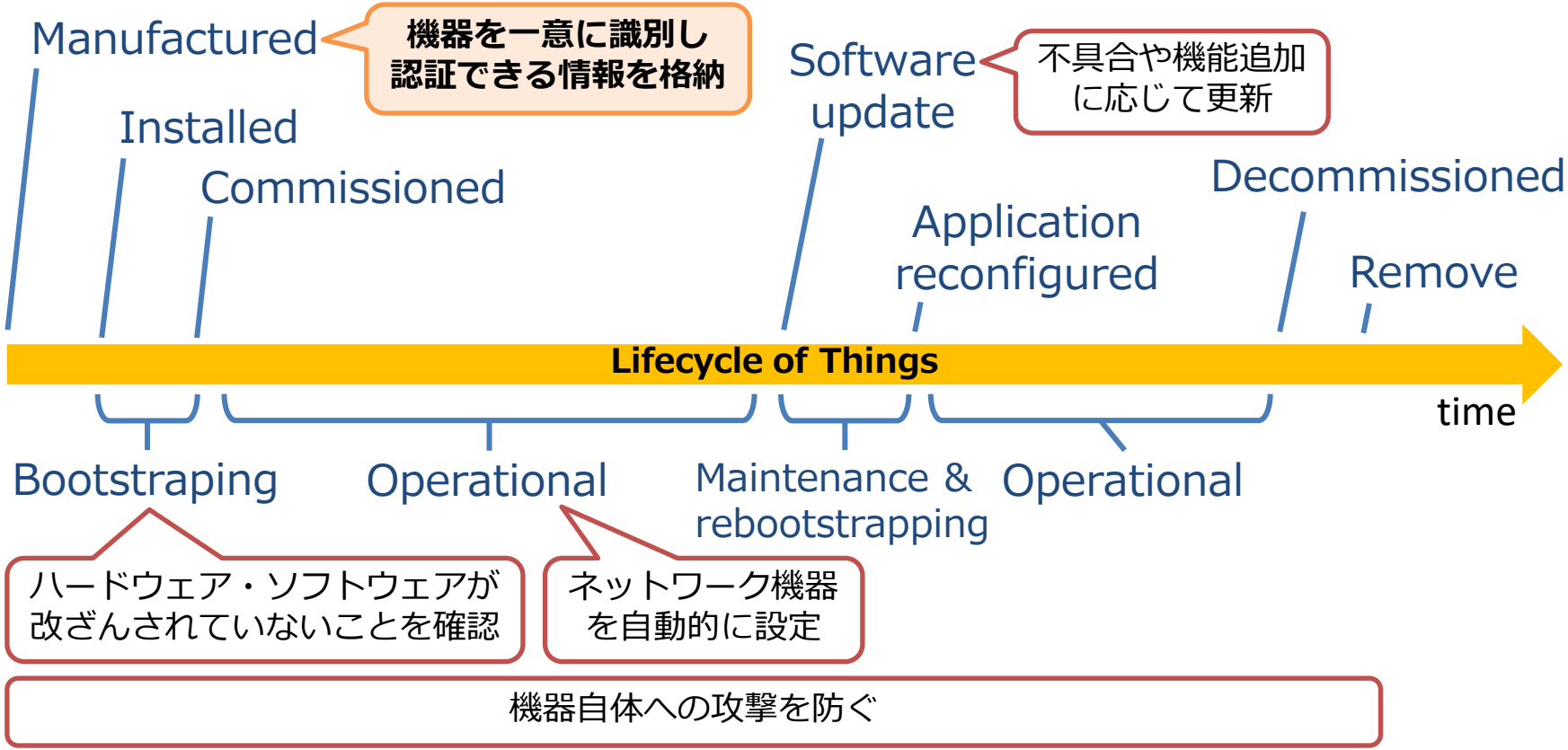
IoTサービスの課題　― 機器のライフサイクル管理 ―



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続けたい

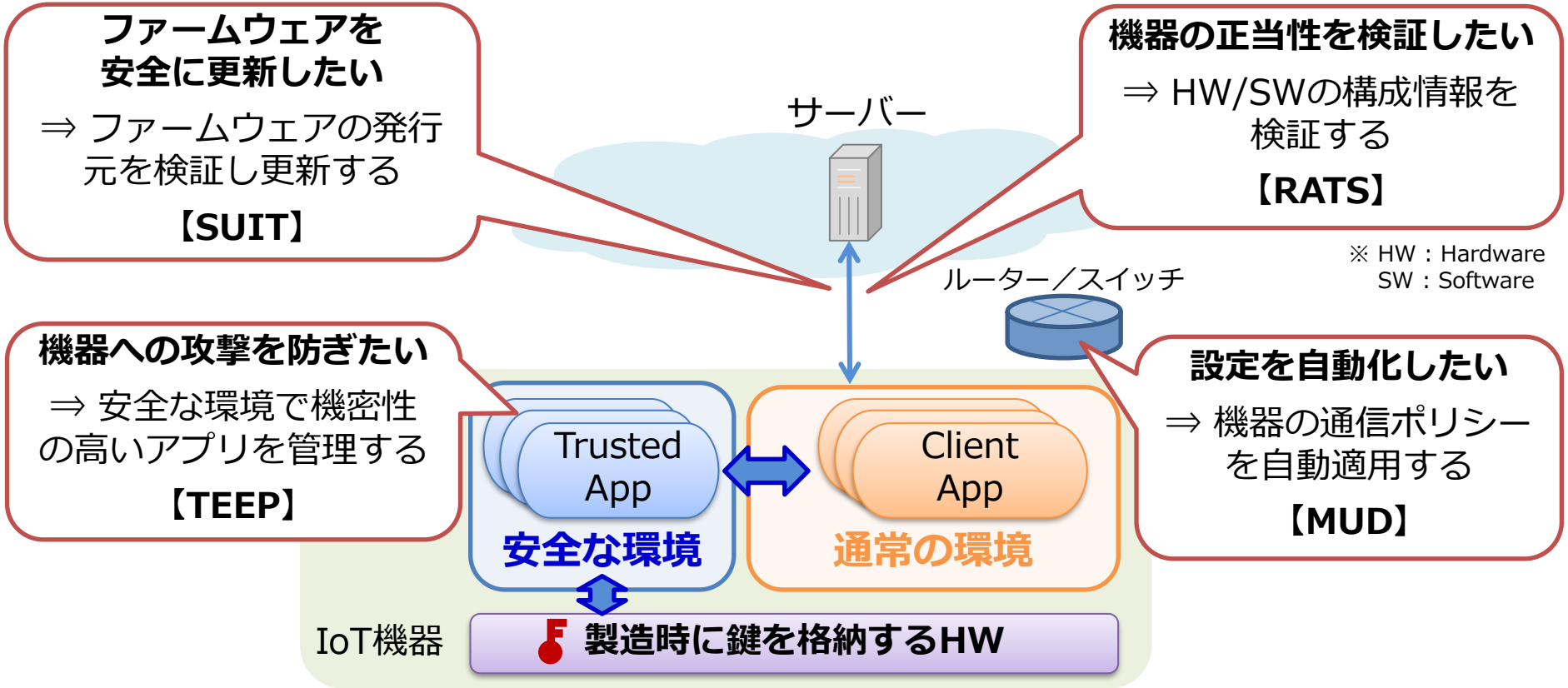
©2020 SECOM CO., LTD.　本発表専用の資料となりますので第三者への開示・転用はお控えください。

IoT機器のライフサイクル管理 ― 時系列で整理 ―



出典：https://tools.ietf.org/html/rfc8576

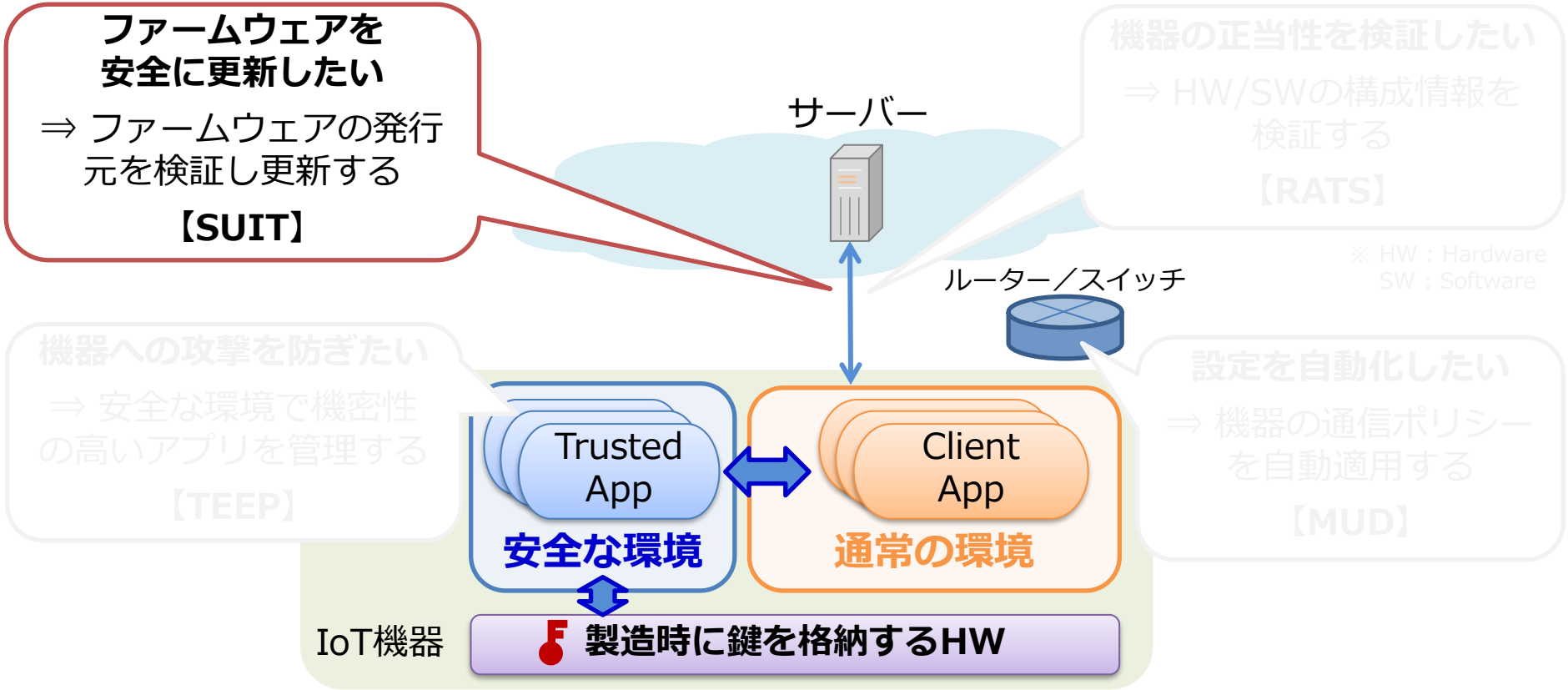
IoT機器のライフサイクル管理　― 標準化が進む技術 ―



目次

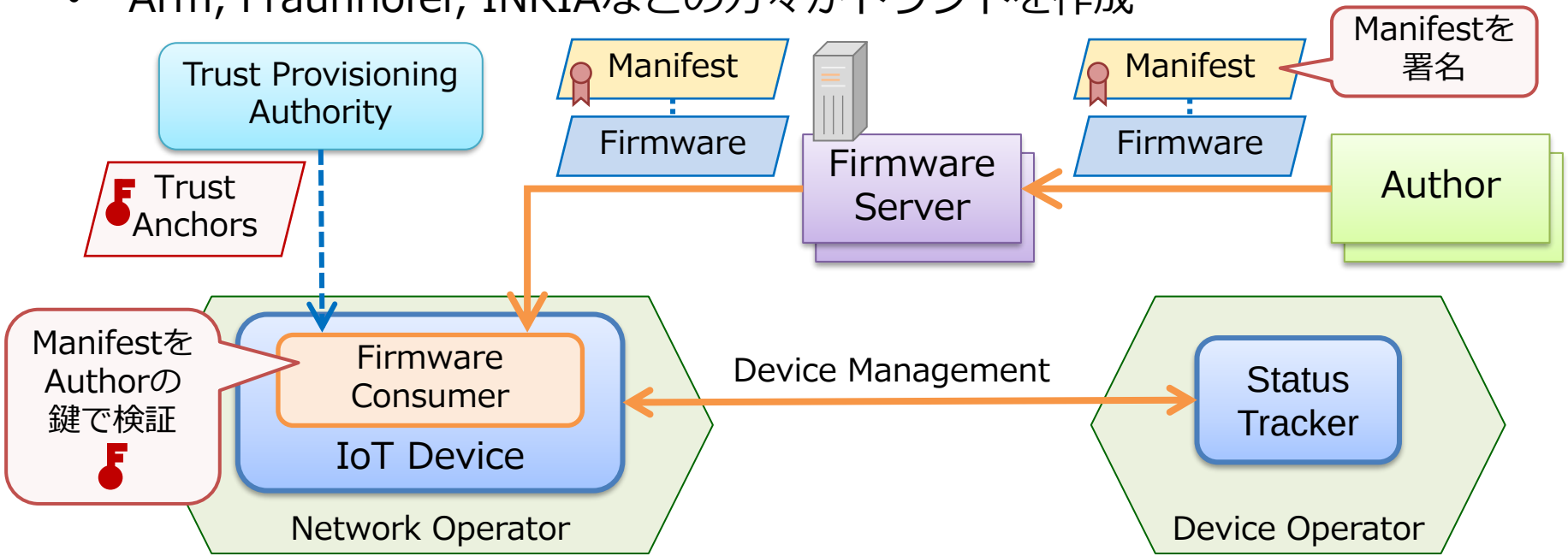
- IoT機器のライフサイクル管理、課題と解決策
- IETFでの国際標準化の動向
- 今後の展望

IoT機器のライフサイクル管理　― 標準化が進む技術 ―



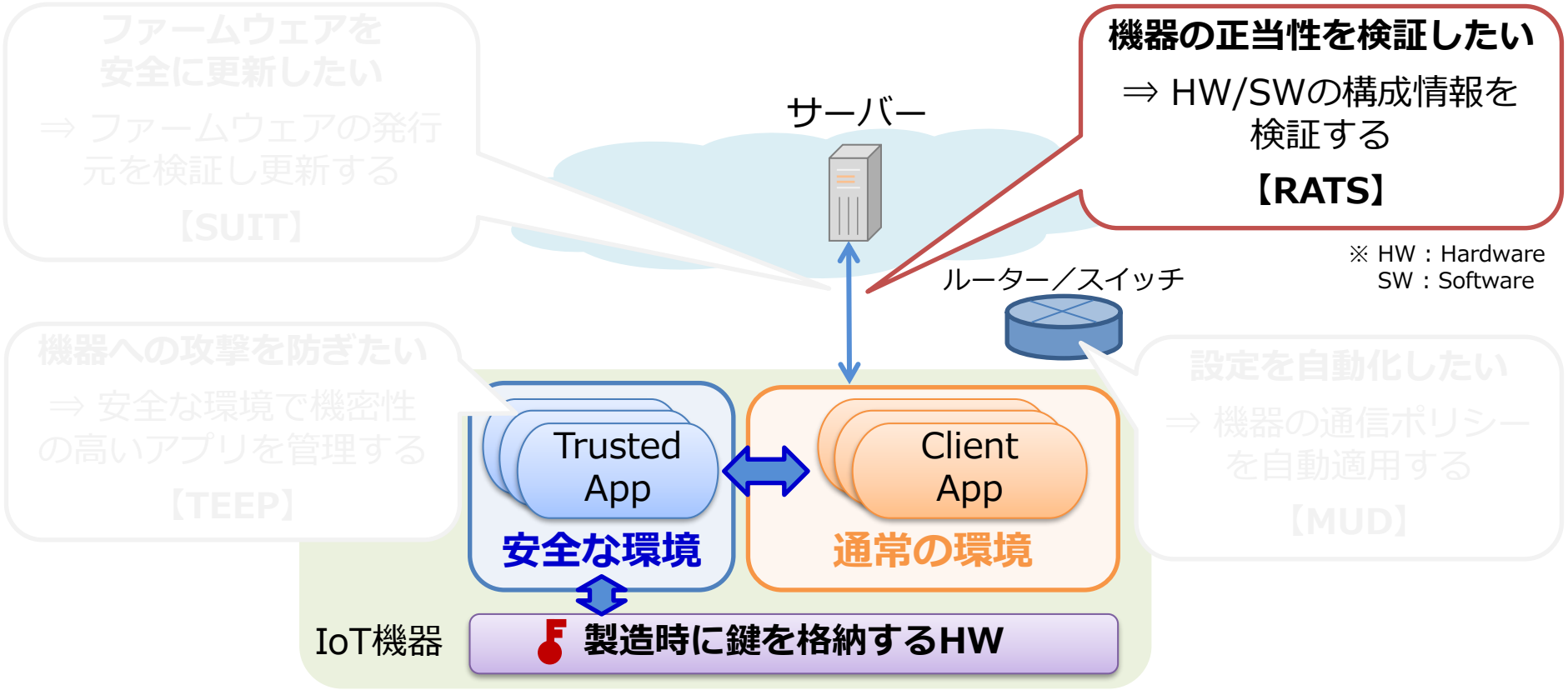
SUIT　IoT機器の安全なファームウェア更新

- SUIT (Software Updates for Internet of Things) WGで検討
- 低リソースな機器 (～10KiB RAM, ～100KiB ROM)を対象とした仕組み
- Arm, Fraunhofer, INRIAなどの方々がドラフトを作成



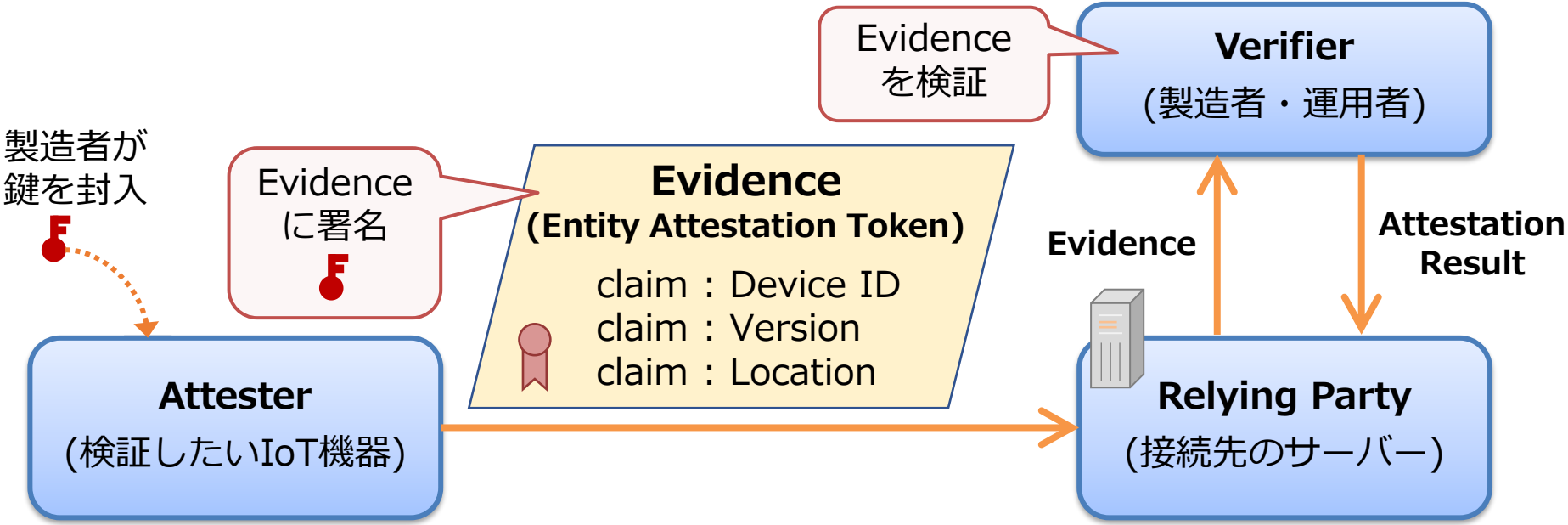
出典：https://tools.ietf.org/html/draft-ietf-suit-architecture-11

IoT機器のライフサイクル管理　― 標準化が進む技術 ―



RATS　IoT機器の正当性の検証

- RATS (Remote ATtestation ProcedureS) WGで検討
- HW/SWの構成が改ざんされていないことを検証する仕組み
- Microsoft, Intel, Qualcommなどの方々がドラフトを作成



出典：https://tools.ietf.org/html/draft-ietf-rats-architecture-04, https://tools.ietf.org/html/draft-ietf-rats-eat-03

©2020 SECOM CO., LTD.　本発表専用の資料となりますので第三者への開示・転用はお控えください。

IoT機器のライフサイクル管理　― 標準化が進む技術 ―

ファームウェアを安全に更新したい

⇒ ファームウェアの発行元を検証し更新する

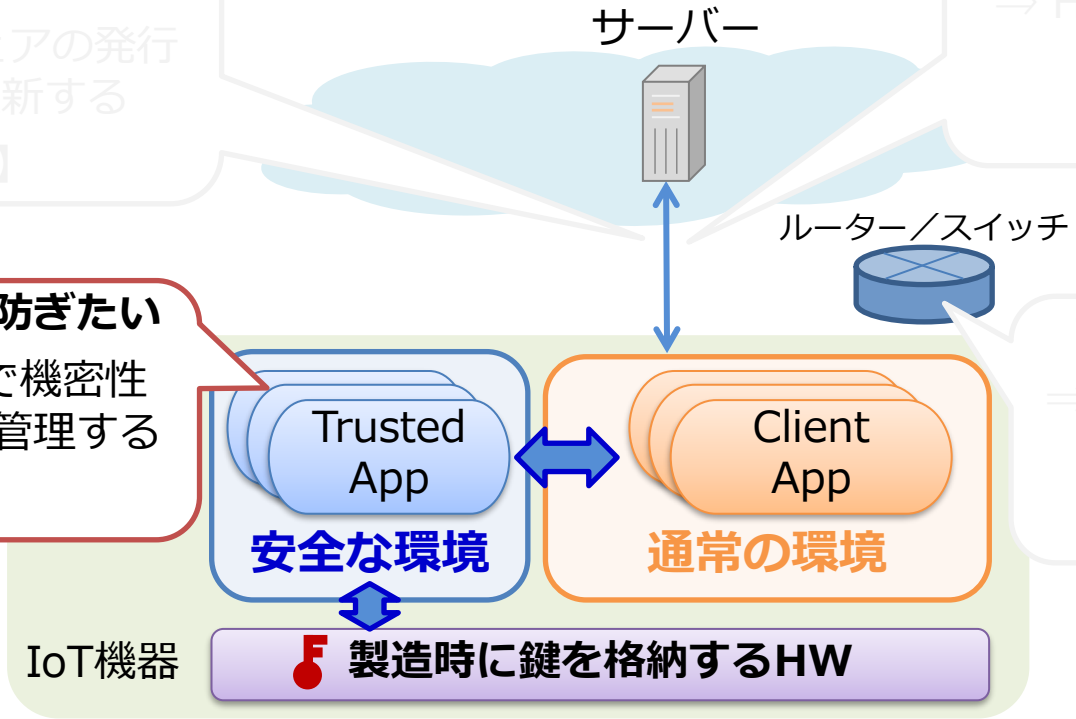
【SUIT】

機器の正当性を検証したい

⇒ HW/SWの構成情報を検証する

【RATS】

※ HW：Hardware
SW：Software



機器への攻撃を防ぎたい

⇒ 安全な環境で機密性の高いアプリを管理する

【TEEP】

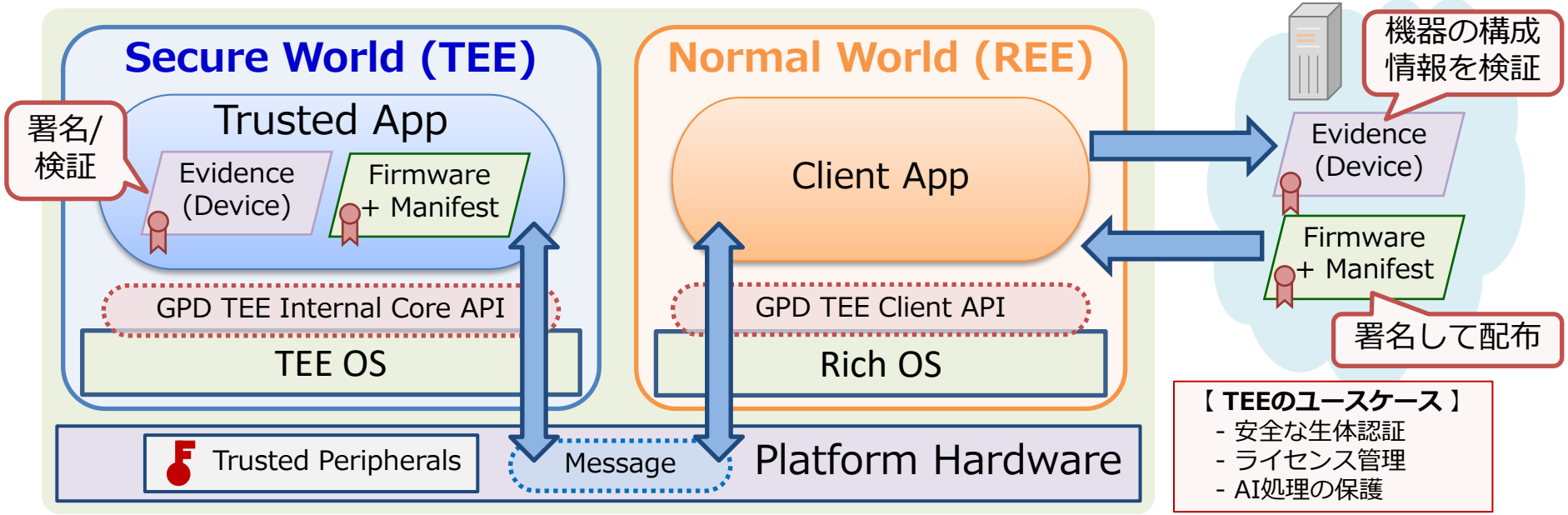
設定を自動化したい

⇒ 機器の通信ポリシーを自動適用する

【MUD】

TEE（Trusted Execution Environment）安全な実行環境

- プロセッサ上に通常の環境とは隔離された安全な実行環境を実現する技術
- TEEの標準化：　ICカードなどの国際標準化を行うGlobalPlatformが推進
- TEEの製品例：　Arm TrustZone、Intel SGX(Software Guard Extensions)など

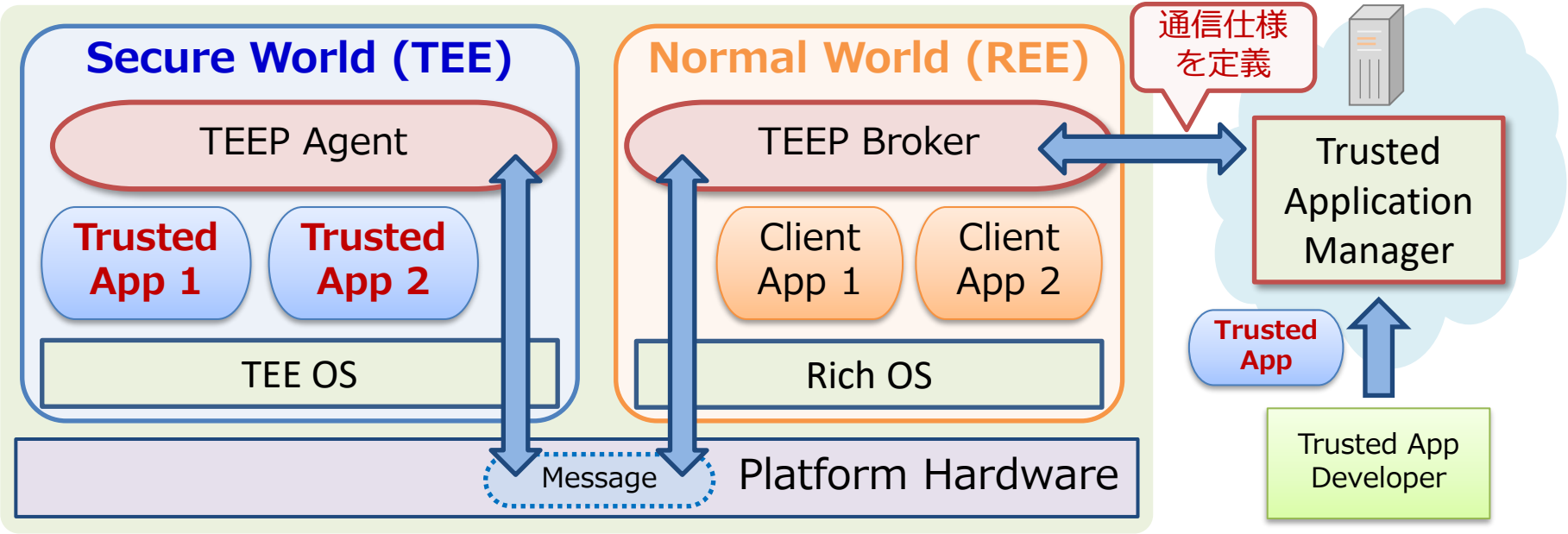


【 TEEのユースケース 】
- 安全な生体認証
- ライセンス管理
- AI処理の保護

出典：https://globalplatform.org/specs-library/tee-system-architecture-v1-2/　※ REE：Rich Execution Environment, GPD：GlobalPlatform Device committee

TEEP　機密性の高いアプリケーションの遠隔管理

- TEEP (Trusted Execution Environment Provisioning) WGで検討
- 安全な実行環境のアプリ（Trusted Application）を管理するための仕組み
- Arm, Intel, Microsoft, Symantecなどの方々がドラフトを作成



出典：https://tools.ietf.org/html/draft-ietf-teep-architecture-09

©2020 SECOM CO., LTD.　本発表専用の資料となりますので第三者への開示・転用はお控えください。

IoT機器のライフサイクル管理　― 標準化が進む技術 ―

ファームウェアを安全に更新したい

⇒ ファームウェアの発行元を検証し更新する

【SUIT】

機器の正当性を検証したい

⇒ HW/SWの構成情報を検証する

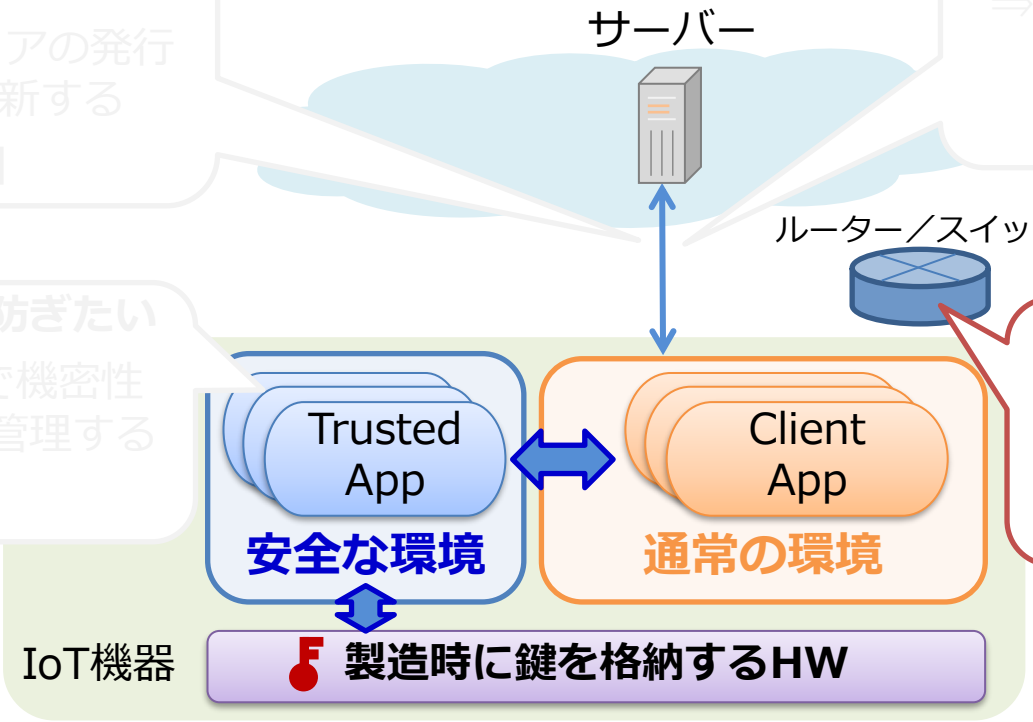
【RATS】

※ HW：Hardware
SW：Software

機器への攻撃を防ぎたい

⇒ 安全な環境で機密性の高いアプリを管理する

【TEEP】



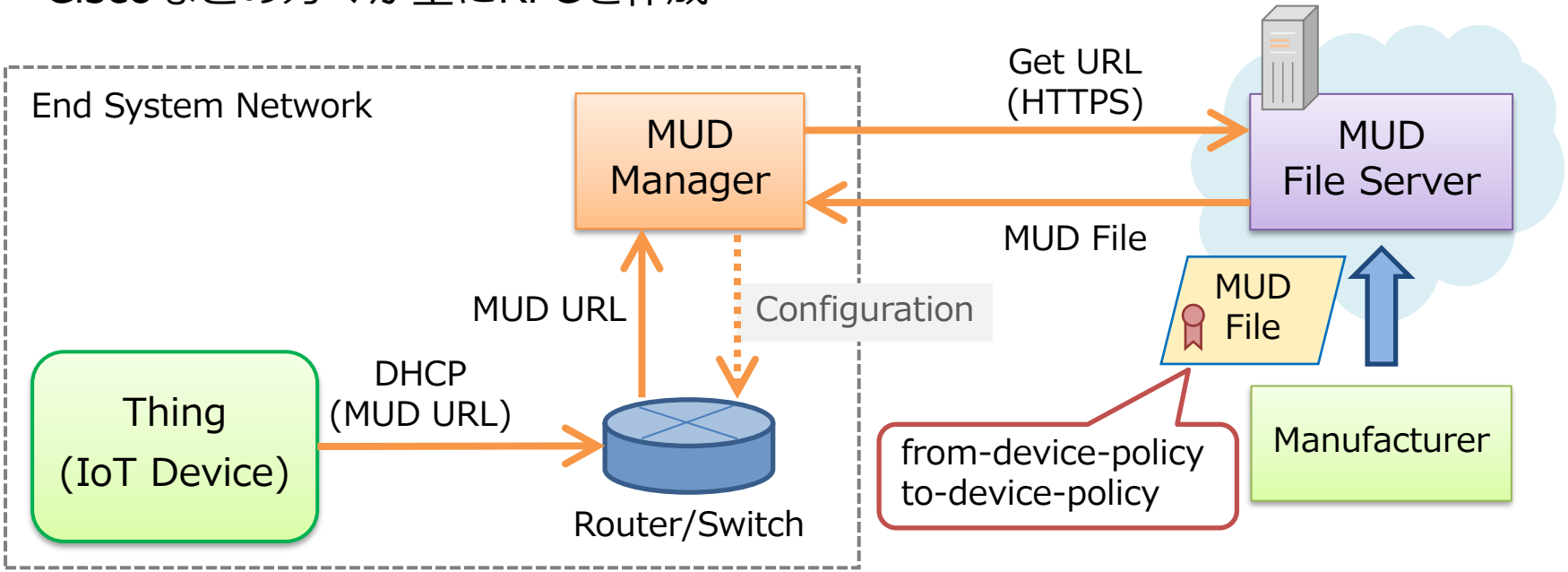
設定を自動化したい

⇒ 機器の通信ポリシーを自動適用する

【MUD】

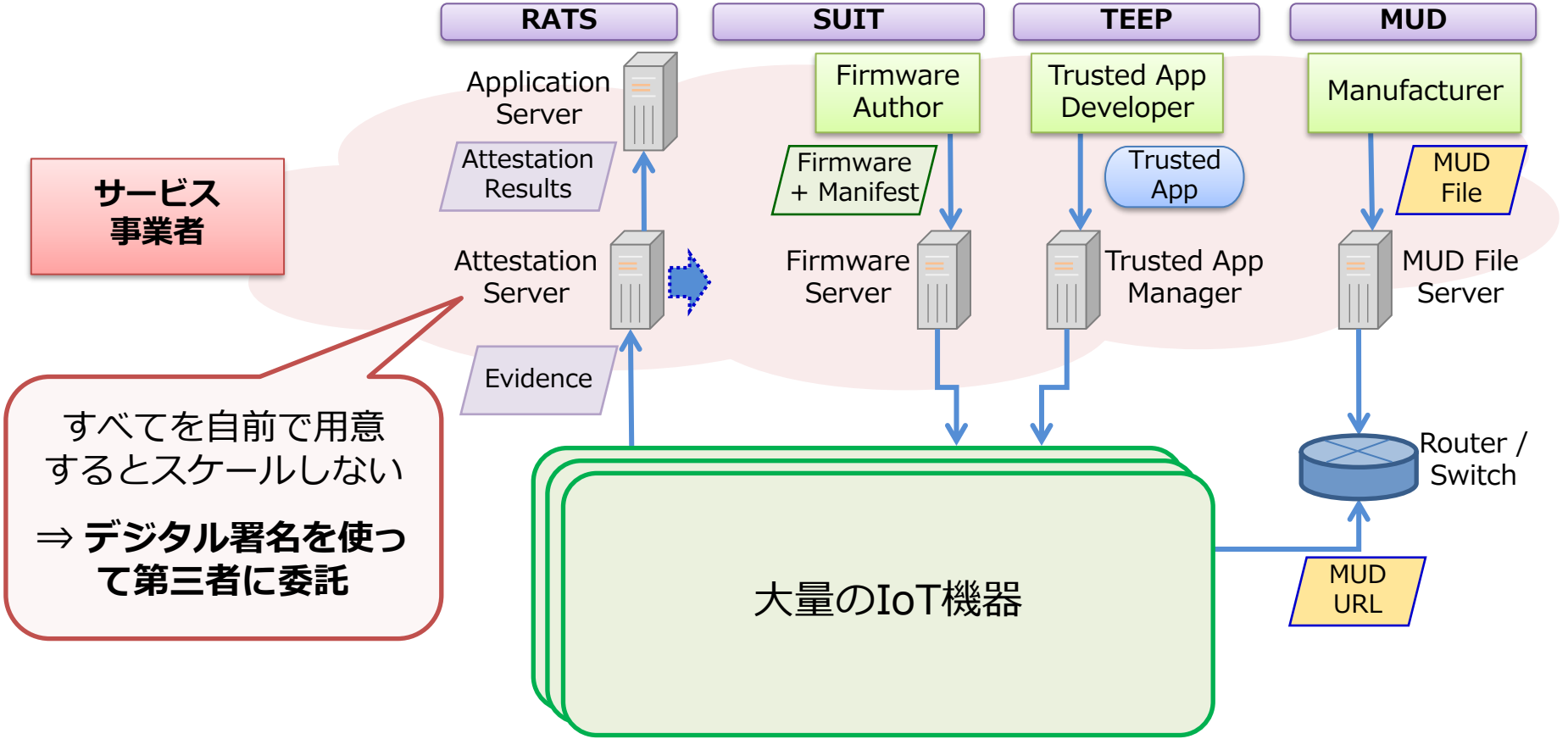
MUD　IoT機器の安全なネットワーク接続

- RFC 8520 - Manufacturer Usage Description Specification として標準化
- IoT機器の通信ポリシーをネットワーク機器に自動的に適用する仕組み
- Ciscoなどの方々が主にRFCを作成

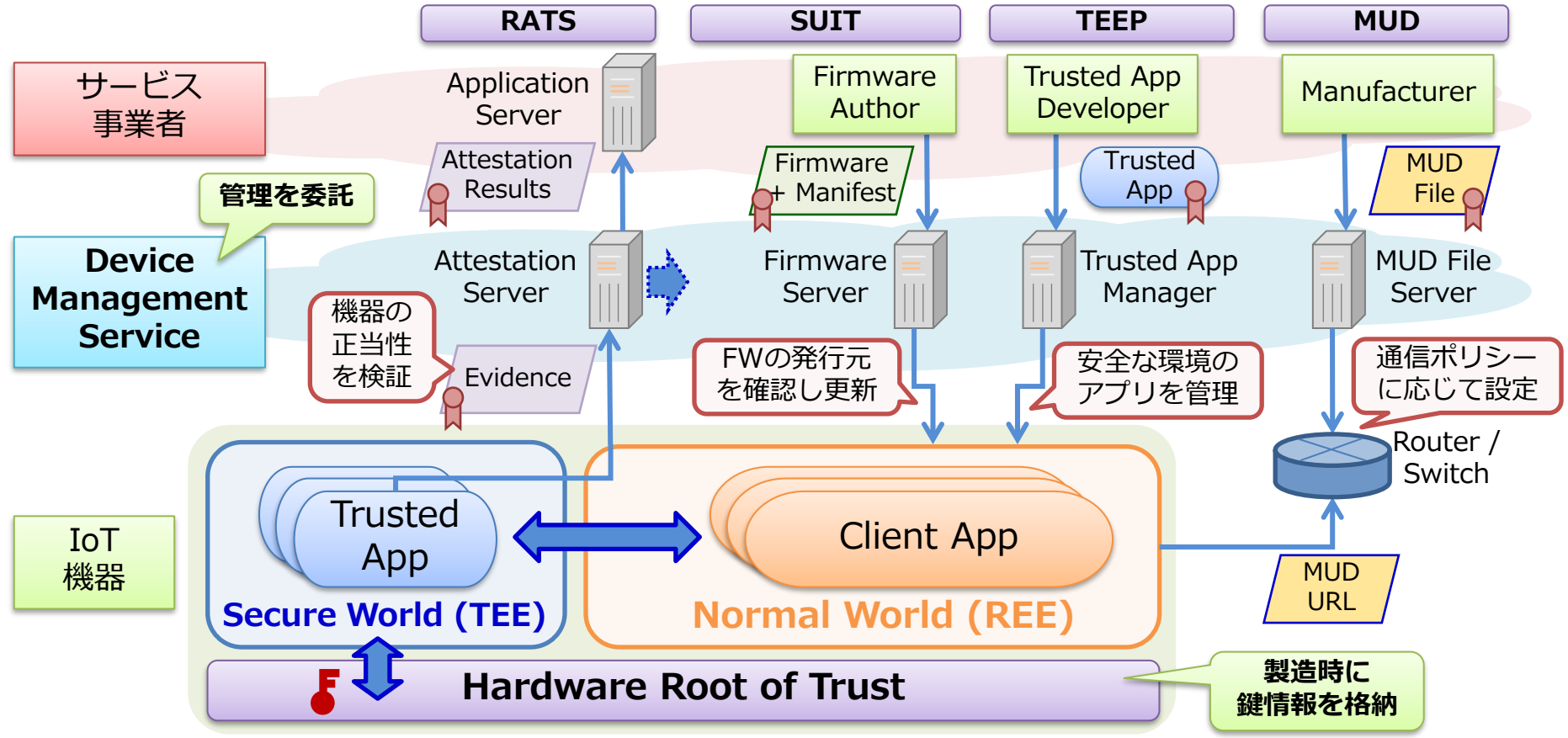


出典：https://tools.ietf.org/html/rfc8520

ライフサイクル管理の標準化の意義　スケールの視点



IoT機器の安全なライフサイクル管理 ― 全体像 ―



IETFの標準化に対する日本からの取り組み　Hackathon

信頼される安心を、社会へ。
SECOM

SUIT

IETF 103

IETF 104

Arm, INRIA, Microsoft, SECOM, …

TEEP

IETF 106

AIST, Arm, Cisco, Microsoft, SECOM

MUD

IETF 105

IETF 106

Cisco, NIST, SECOM, …

出典：
https://datatracker.ietf.org/meeting/103/materials/slides-103-suit-hackathon-report-00
https://datatracker.ietf.org/meeting/104/materials/slides-104-suit-hackathon-report-01
https://www.nccoe.nist.gov/sites/default/files/IETF-Hackathon-MUD-and-Onboarding.pdf
https://github.com/IETF-Hackathon/ietf106-project-presentations/blob/master/IETF106-Hackathon-MUD.pdf
https://github.com/IETF-Hackathon/ietf106-project-presentations/blob/master/ietf-106-hackathon-presentation-teep-20161117-02.pdf

©2020 SECOM CO., LTD.　本発表専用の資料となりますので第三者への開示・転用はお控えください。

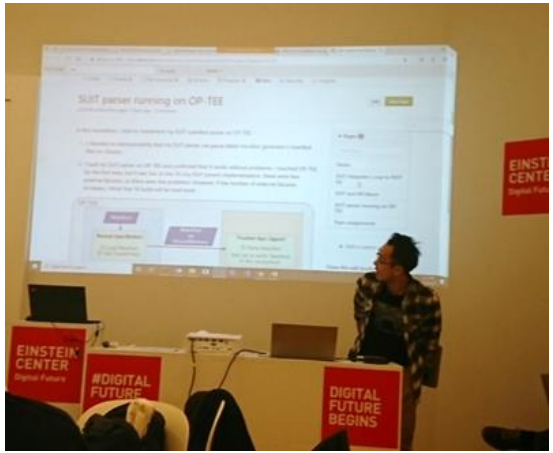
目次

- IoT機器のライフサイクル管理、課題と解決策
- IETFでの国際標準化の動向
- 今後の展望

Hackathonの多様化　IETF外での開催

- **イベント名称：** Securing the IoT Hackathon 2020
- **サポーター：** Arm, Einstein Center Digital Future, Nordic Semiconductor, RIOT
- **開催日：** 2020年2月17日 – 19日（Tutorial 1日間、Hackathon 2日間）
- **場所：** ドイツ、ベルリン、Einstein Center Digital Future
- **目的：**
  ① SUIT / TEEP / RATSの実装に取り組み、結果を標準化にフィードバック
  ② 前記技術の初学者を対象とした講習
- **結果：**
  – 参加者は35名程度（途中増減あり）
  – 人数比：IETF ＞ OSS ＞ 大学や個人
  – 企業・OSSコミュニティ・大学が連携し標準化活動を広めていく熱意を感じた

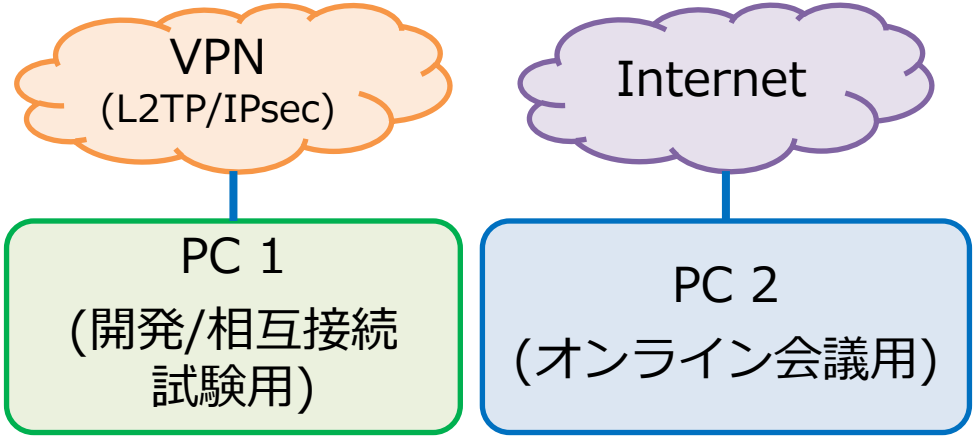
併催のSUIT Virtual Interim Meetingで成果を発表 ↓



Hackathonの多様化　オンライン開催

- **イベント名称：** TEEP Virtual Hackathon
- **参加者の所属：** AIST(主催), Lepidum, Microsoft, Roboc, TRASIO, SECOM（10名）
- **開催日：** 2020年3月27日（Hackathon 1日間）
- **場所：** 自宅から参加
- **目的：**
  ① Virtual Hackathonの環境整備
  ② TEEPの仕様を実装し結果をWGにフィードバック
- **結果：**
  – リモート環境で協力して実装するための知見を得ることができた
  – 事前準備は現地開催よりも十分に必要
  – 情報共有の増加という利点があった

Virtual Hackathonにおける自宅の参加環境



©2020 SECOM CO., LTD.　本発表専用の資料となりますので第三者への開示・転用はお控えください。

IoTセキュリティの議論の拡大

- IETF 106でのSide Meetingで「**IoT Systems WG** 」が提案される
  - 複数のSDOを跨いで議論を積み上げていきたい
  - それぞれの要求に関する、ギャップと重複に注目する
    - 例：Wi-Fi Alliance DPP (Device Provisioning Protocol) と IETF MUD
  - 必要に応じて、Architectural Documentsを作成する
  - 最初は、**IoT Onboarding**に関する議論から始める
- WG設立の議論は継続

※ SDO： Standards Development Organizations
IoT Onboarding： IoT機器を導入する際の準備から立ち上げまでの作業

©2020 SECOM CO., LTD.
本発表専用の資料となりますので第三者への開示・転用はお控えください。

IoTセキュリティに関するIETFでの国際標準化　まとめ

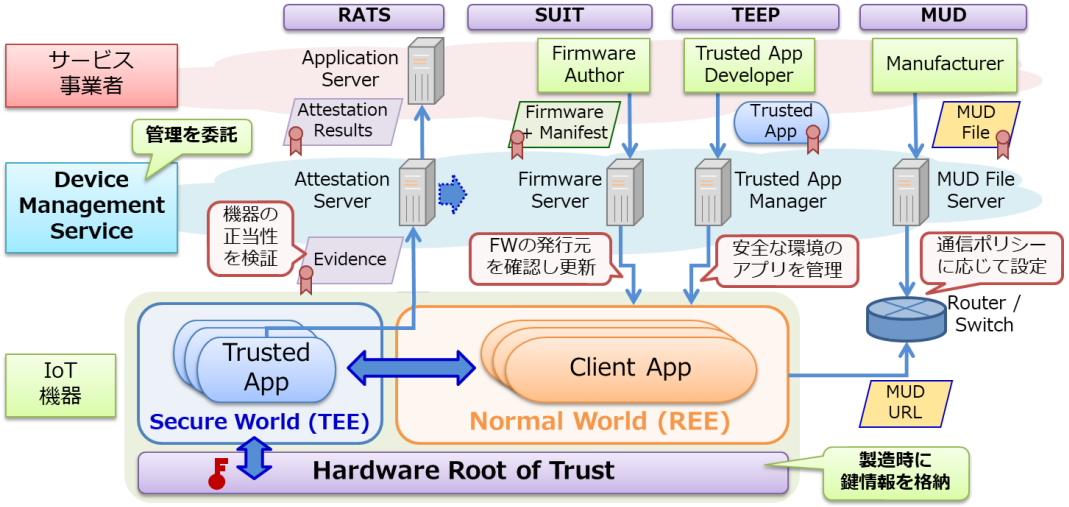
- **IoT機器のライフサイクル管理、課題と解決策**
  - ファームウェアを安全に更新したい：　SUIT
  - 機器の正当性を検証したい：　RATS
  - 機密性の高いアプリを管理したい：　TEEP
  - 機器の通信ポリシーを自動適用したい：　MUD

  遠隔から長期間・安全に管理

- **IETFでの国際標準化の動向**
  - デジタル署名を利用して、機器の管理を第三者に委託

  ⇒ サービス事業者の負担軽減＆大規模にスケールできる

- **今後の展望**
  - 多様化するHackathonの形態
  - IoTセキュリティの議論の拡大



以下、補足資料

©2020 SECOM CO., LTD.
本発表専用の資料となりますので第三者への開示・転用はお控えください。

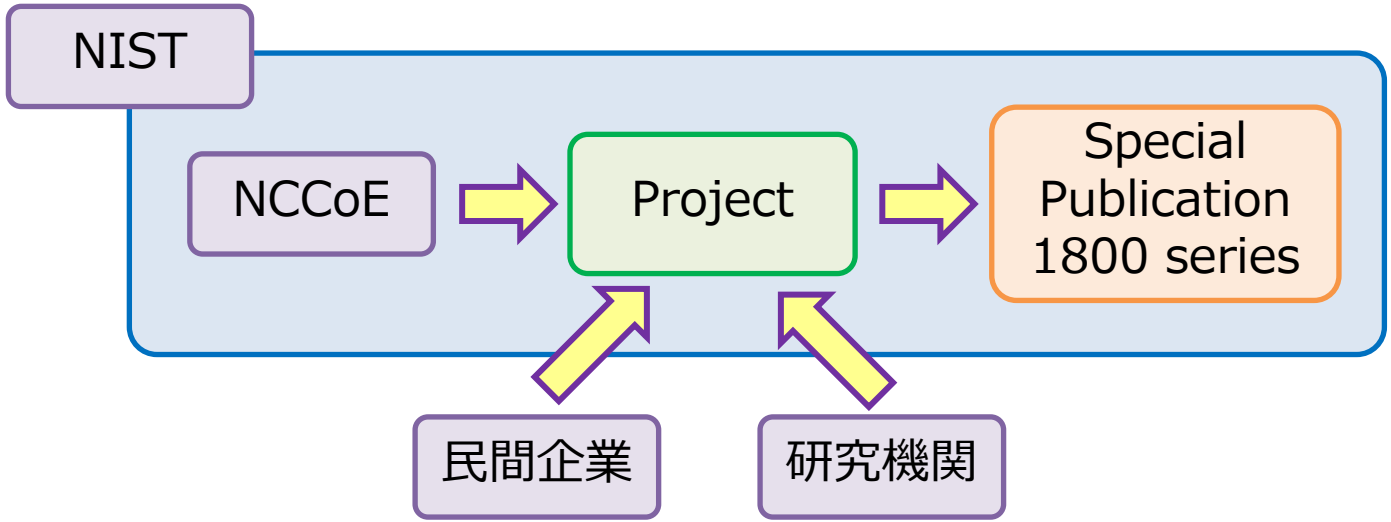
IETF Hackathonとは

- **概要**
  - IETF標準の実装について、参加者による共同開発や議論を行うイベント
- **開催の目的**
  - IETFの標準化活動の加速
  - IETFの活動への関心を広げるため
- **特徴**
  - IETF 92（2015年）から開催
  - IETFの始め2日間で実施（土、日）
  - 参加者はプロジェクトを選択して参加
  - プロトコルの実装や相互接続試験などに取り組む

出典：https://www.ietf.org/blog/third-hackathon-prague/

MUDの標準化を取り巻く動向　NIST NCCoEとは

- 2012年、NISTは産学官連携の研究開発センターとしてNCCoEを設立
  - Cisco, IBM, Intel, Juniper, Microsoftなどの企業が協力
  - サイバーセキュリティ技術を普及させることが目的

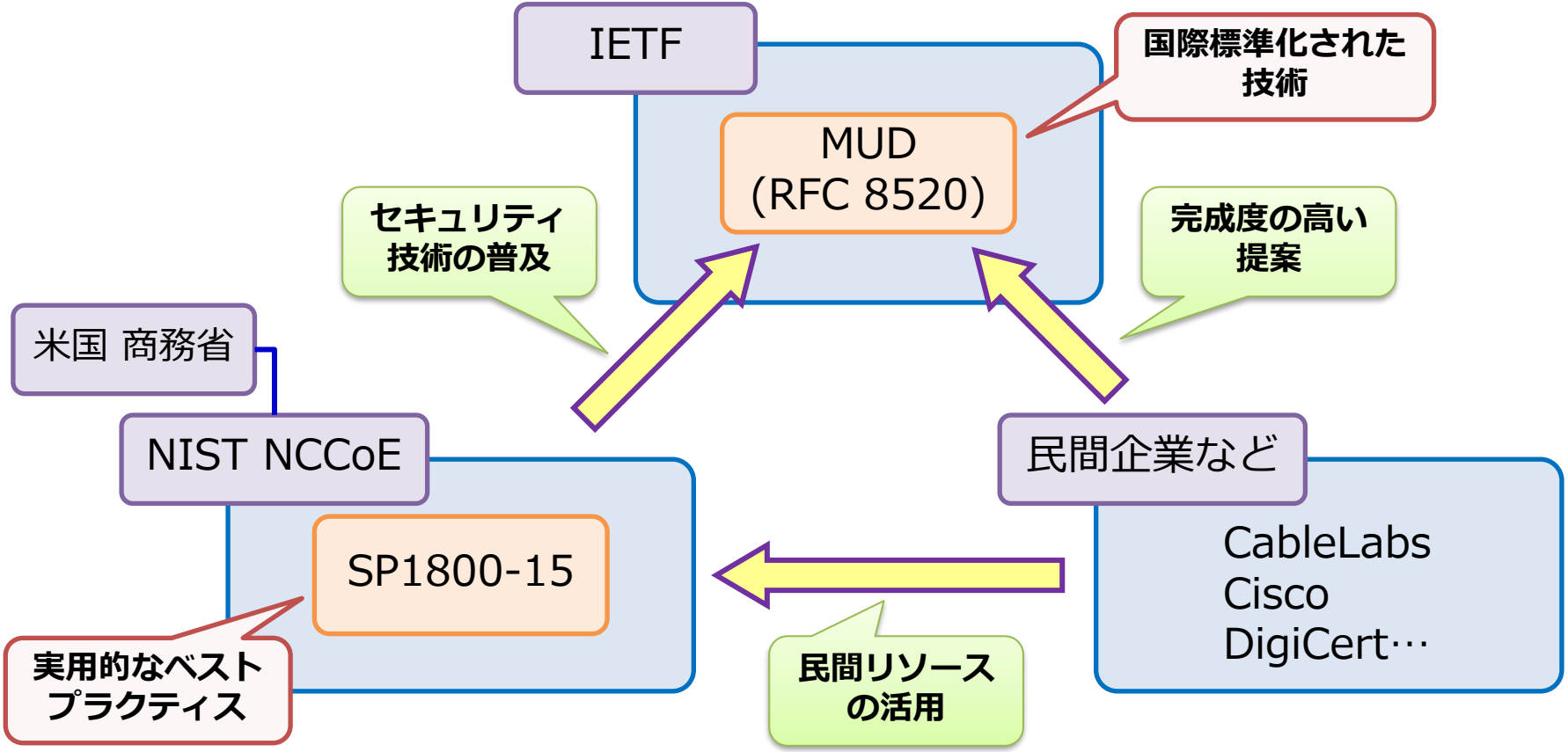


※ NIST：　National Institute of Standards and Technology
NCCoE：National Cybersecurity Center of Excellence

MUDの標準化を取り巻く動向　NIST SP1800-15の発行

- **目的**
  - 攻撃者がIoT機器を乗っ取った場合の有用性を制限することで、ボットネットに関する脆弱性を低減する
- **スコープ**
  - ホームおよびビジネスネットワークにおけるIoT機器の安全なデプロイメントに関する提案手法
  - 新しい標準技術をIoT機器とネットワーク機器に適用して、マルウェアを制限
  - MUD（RFC8520）を使用する
- **発行**
  - 2019年　4月　1st　Draft
  - 2019年11月　2nd Draft

IETF MUD (RFC 8520) は、2019年3月に発行

出典：https://csrc.nist.gov/publications/detail/sp/1800-15/draft

MUDの標準化を取り巻く関係者の構図（考察）