PKI 相互運用技術WGの活動における標準化との関わり

2021年1月15日

JNSA標準化部会 副部会長/ PKI相互運用技術WGリーダ
松本　泰　（セコム株式会社IS研究所）

PKI 相互運用技術WGの活動における標準化との関わり

- IETF
  - 2002年-2008年
    - 2001年に開始したChallenge PKIプロジェクの成果をIETF PKIX WG へ
  - 2008年
    - RFC 5217 Memorandum for Multi-Domain Public Key Infrastructure Interoperability　発行
    - https://tools.ietf.org/html/rfc5217
  - 2017年以降
    - IETFのIoTセキュリティ関係の活動に着目
    - オープンなセミナー「PKI day」やWG内のIETF報告会などで、その動向を情報共有
- 暗号鍵管理勉強会　2020年
  - NIST SP 800-130 A Framework for Designing Cryptographic Key Management Systems」、CRYTPREC 暗号鍵管理システム設計指針（基本編）を題材とした勉強会を開催

Challenge PKI Project

The Multidomain PKI Interoperability Framework

Japanese
English

出典：
https://www.jnsa.org/mpki/index.html

Contents

- What's new?
- Introduction
- Projects
- Conferences
- Contact
- Partners

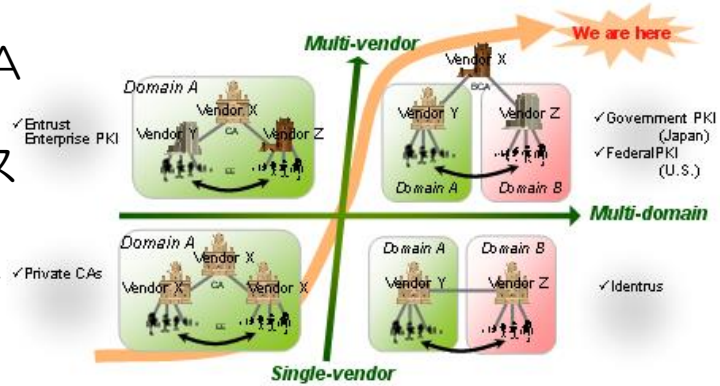
What's new?

- Our Proposal Memorandum for Multi-domain PKI Interoperability is now published as RFC 5217. (July 2008) NEW!
- The testcase database for Timestamp Protocol Interoperability Test Suite is downloadable. (July 2004)
- The testcase database for CPKI-TS 2
Government PKI (GPKI), Local Gover
2004)
- The brand-new version of Challenge
- The online test center for Timestamp
- We have issued an announcement abo
conclusion of the 58th IETF discussion

Introduction

According to the development of e-government and e-commerce, the importance of PKI (Public Key Infrastructure) has been growing. A small minority of PKI vendors were the main player and PKI was used in closed domain in early PKI. There are many players around PKI and multiple PKI domains are cross connected in these latter days (e.g. GPKI in Japan, U.S. Federal PKI).

- 「Challenge PKIプロジェク」は、NPO JNSAが、2001年に開始したプロジェクト
- マルチドメインPKIのための標準化活動や、テストスイートなどの開発を行なってきた。
- 開始から20年経った2021年現在、マルチドメイン・マルチステークホルダー間のトラストの確立、及び、相互運用性の確保は、Society5.0的課題



Transition of PKI models

PKI day 2019 までの歩み

1	2005	PKI技術最新事情	技術中心の議論
2	2006	PKIの展開と最新技術動向	
3	2007	PKIの過去・現在・未来	
4	2008	PKIの標準から実装まで 最新動向	
5	2009	さまざまな分野に展開されるPKIの最新動向	
6	2010	社会基盤としてのPKI／PKIの10年	法制度も含めた議論
7	2011	番号制度時代のPKI	
8	2012	・我が国における信頼基盤の連携に向けて ・PKIへの攻撃とその対応	
9	2014	・公開鍵暗号に関連する周辺技術動向の共有 ・デジタル社会のための「電子署名を見直す」	
10	2015	サイバーセキュリティの要となるPKIを見直す	
11	2016	マイナンバー時代のPKI	社会の変化に伴う議論??
12	2017	IoT・ブロックチェーン時代のPKI	
13	2018	超スマート社会（Society 5.0）におけるトラストの在り方	
14	2019	午前の部　IoTのトラスト 午後の部　トラストサービスの在り方	

出典：
PKI Day 2019
2019年4月17日
https://www.jnsa.org/seminar/pki-day/2019/data/190417_am05_matsumoto.pdf

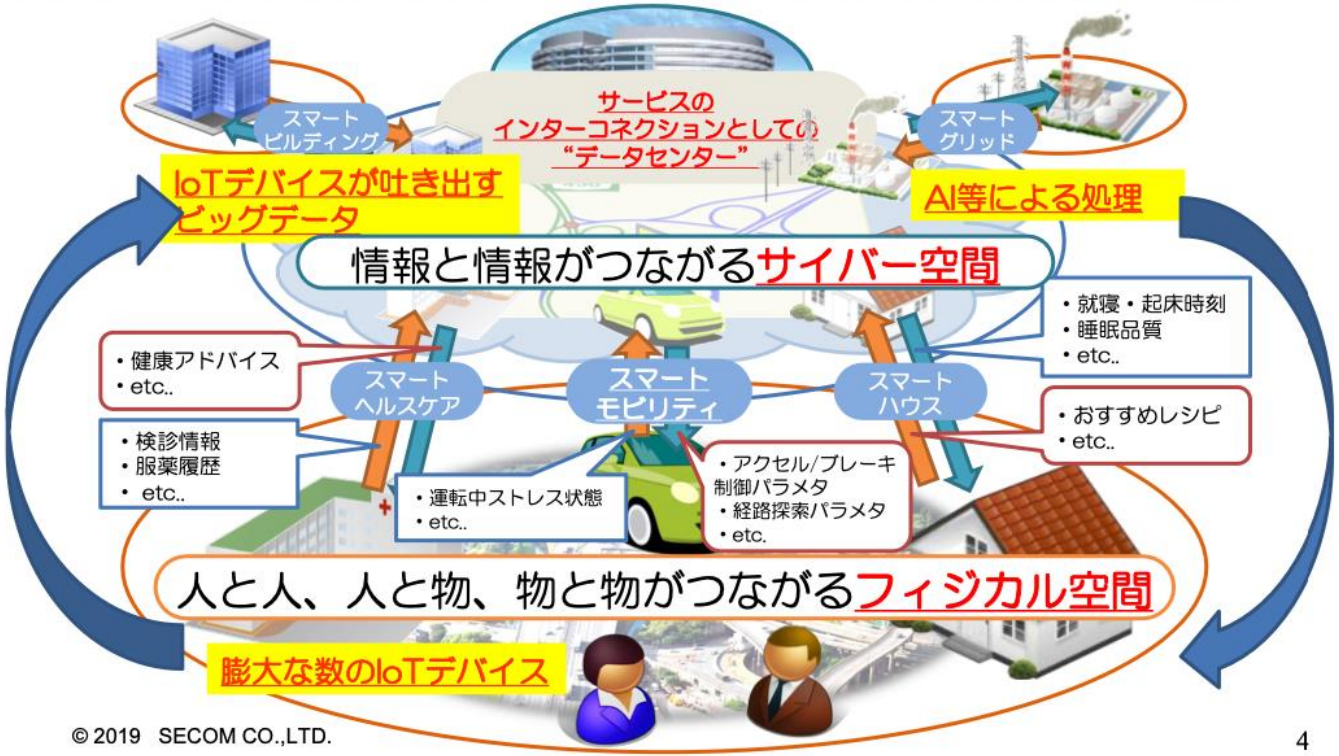
IoT,CPS（cyber physical systems）のトラスト確立のためのIETF等の標準化動向に注目

セコムIS研究所 Intelligent Systems Laboratory

JNSA

午前中の部　IoTのトラスト

IoTサービスシステム ≒　CPS（Cyber Physical Systems）

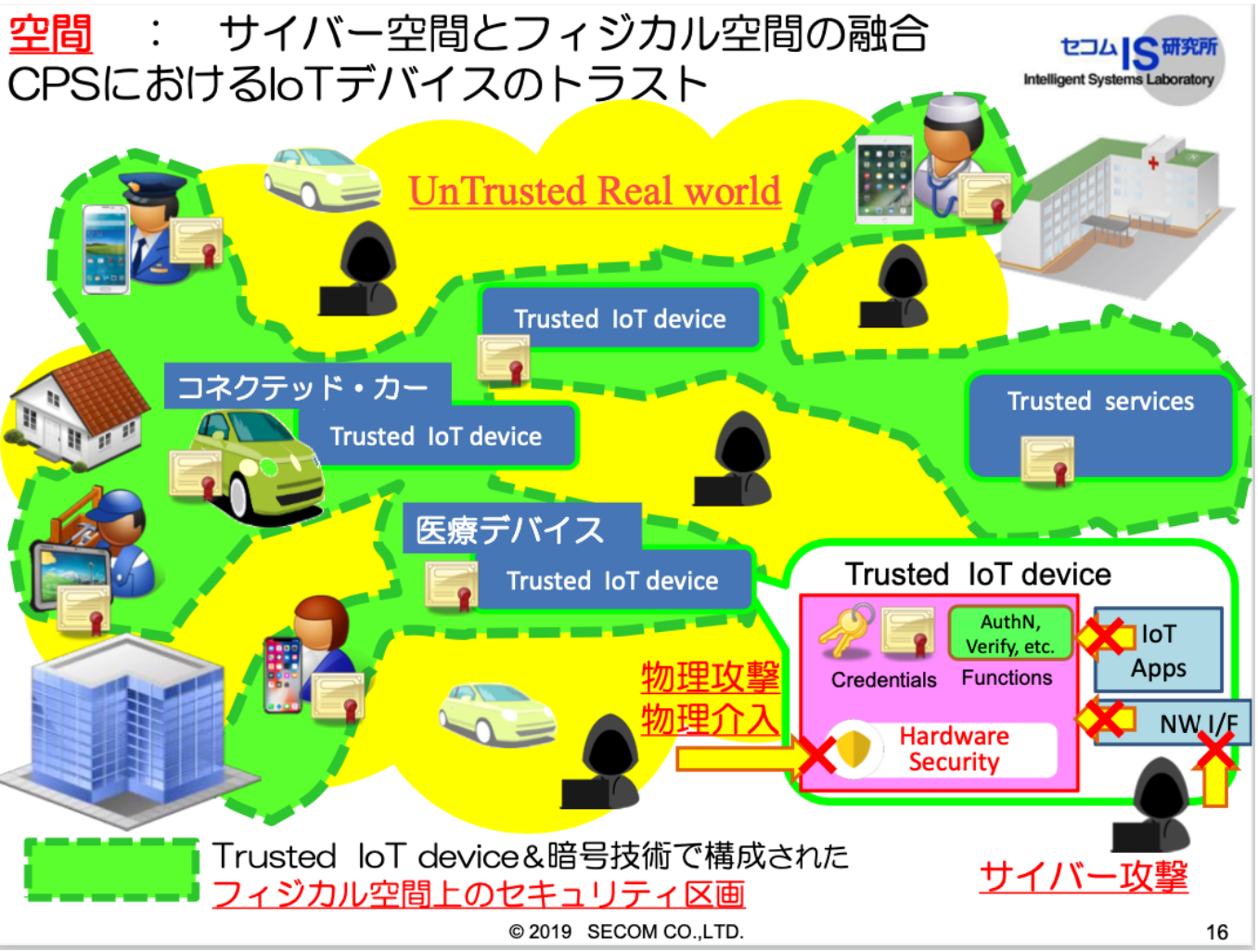


4

出典：
PKI Day 2019
2019年4月17日
https://www.jnsa.org/seminar/pki-day/2019/data/190417_am05_matsumoto.pdf

society5.0時代に必要となるCyber Physical Systems（CPS）は、

AI　＋
BigData　＋
Trusted IoT devices
などが重要

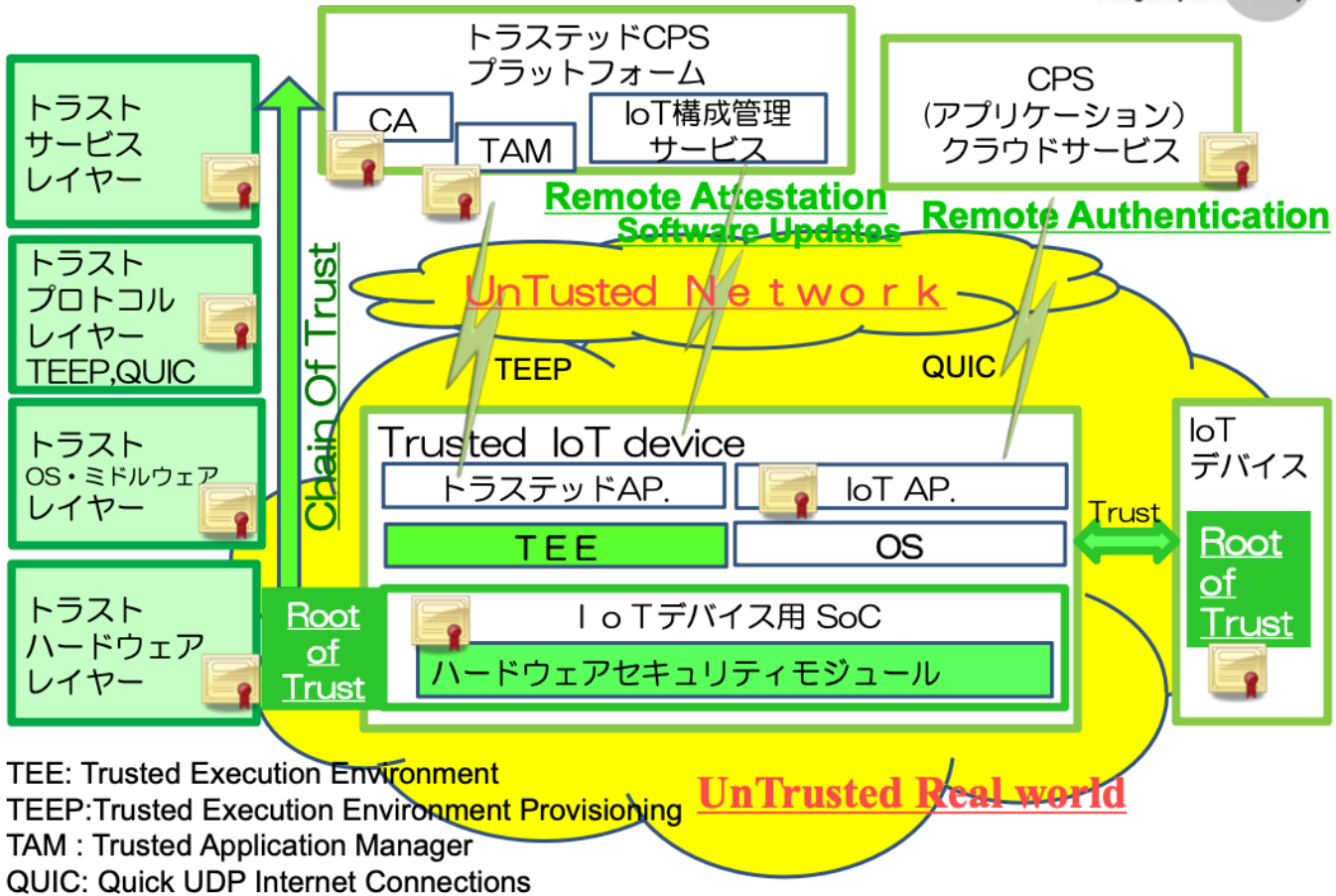


出典：
PKI Day 2019
2019年4月17日
https://www.jnsa.org/seminar/pki-day/2019/data/190417_am05_matsumoto.pdf

Trusted IoT devicesは、ゼロトラストネットワークでは、“untrusted networks”において利用されるデバイスとして期待される。

Cyber Physical Systems (CPS)では、“Untrusted real world”において利用されるデバイスとして期待される。

トラストなCPSのレイヤー構造



出典：
PKI Day 2019
2019年4月17日
https://www.jnsa.org/seminar/pki-day/2019/data/190417_am05_matsumoto.pdf

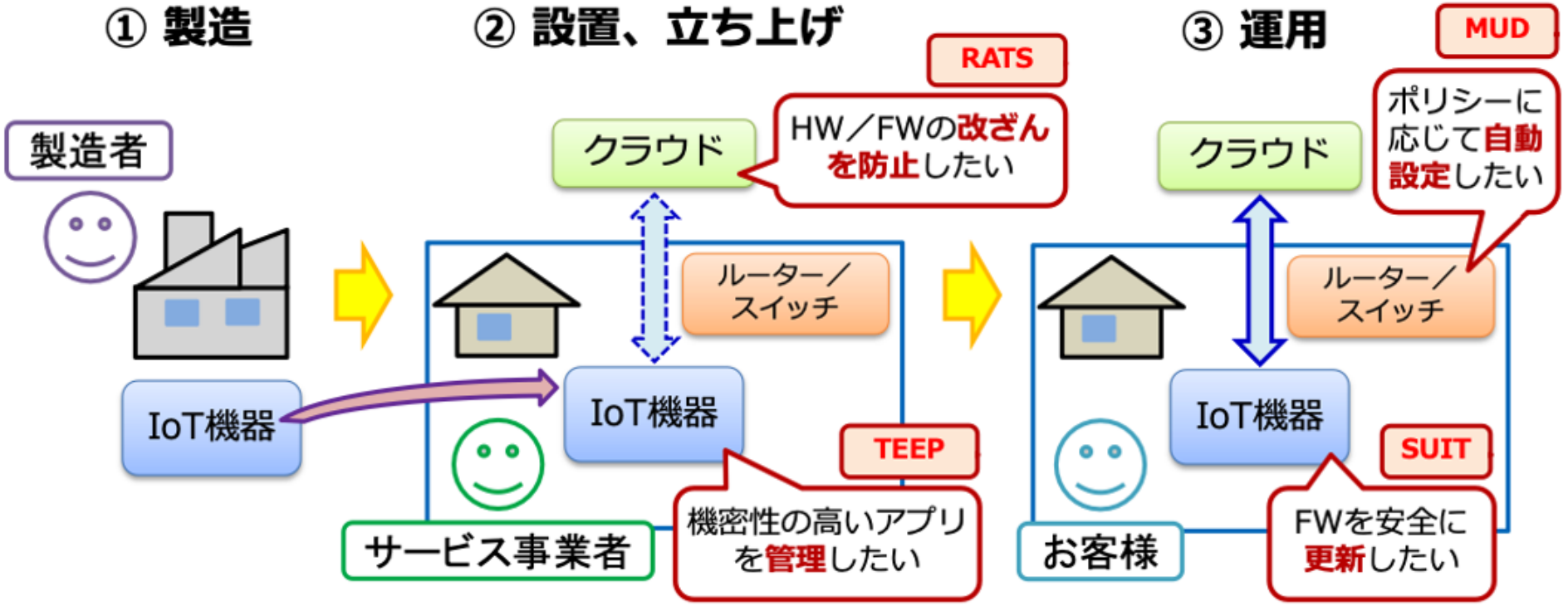
- Cyber Physical Systems (CPS)で利用される膨大な数のTrusted IoT devicesは、クラウドからセキュアに管理される必要がある。
- そのためには、トラストプロトコルレイヤー、トラストサービスレイヤが大きな役割を果たす。

トラストなCPSのレイヤー構造
IETFにおけるIoT・CPSのためのトラスト・プロトコルレイヤーの活動

- SUIT　　Software Updates for IoT
  - https://datatracker.ietf.org/wg/suit/about/
- RATS　　Remote ATtestation ProcedureS
  - https://datatracker.ietf.org/wg/rats/about/
- TEEP　　Trusted Execution Environment Provisioning
  - https://datatracker.ietf.org/wg/teep/about/
- MUD　　Manufacturer Usage Description Specification
  - RFC 8520 Manufacturer Usage Description Specification
    - https://tools.ietf.org/html/rfc8520

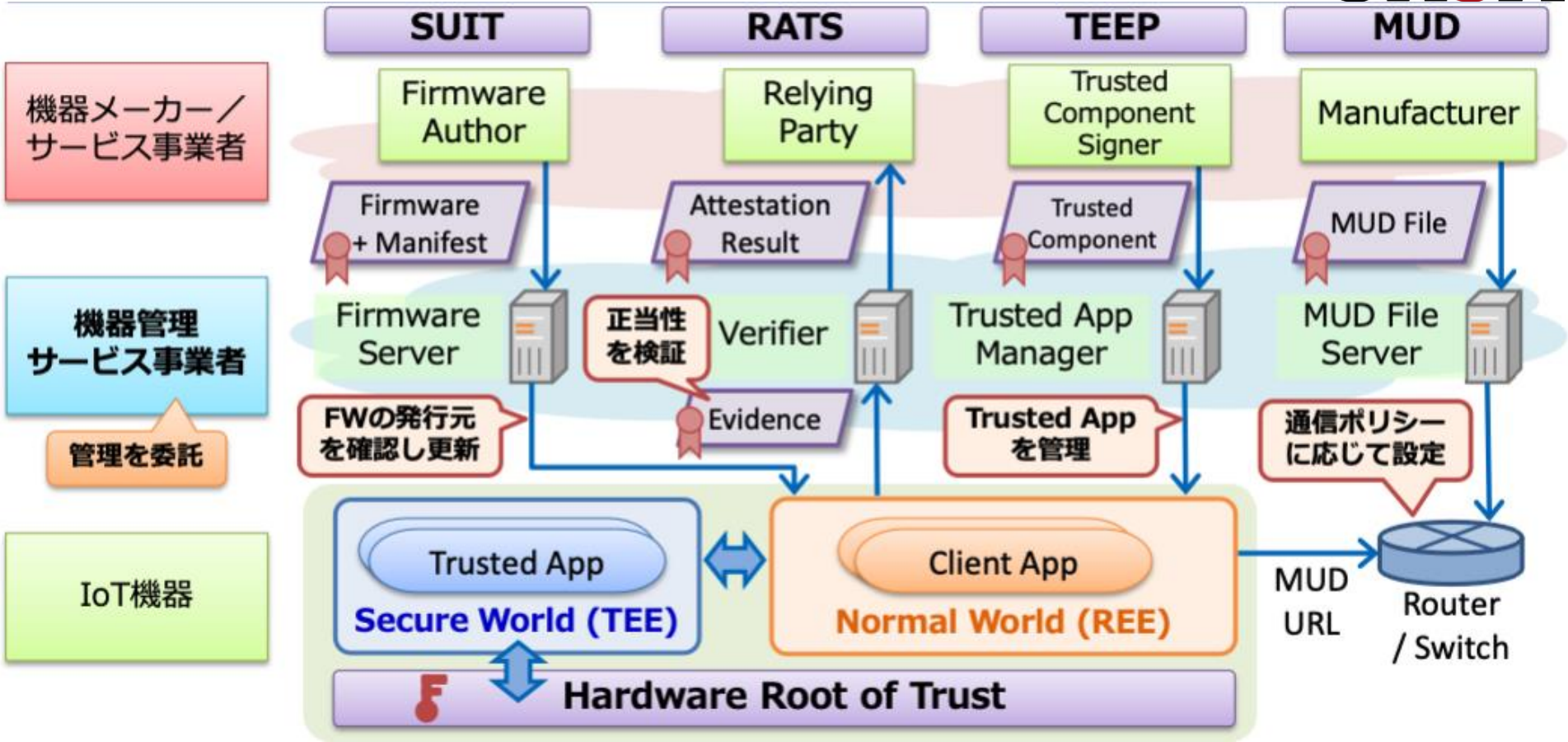
これらのプロトコルの共通点は、ネトワーク中を流れるデータ・オブジェクトにデジタル署名が付されること。PKI&トラスト技術の観点からは、この「デジタル署名」のLoA（Level of Assurance）などの署名ポリシーが非常に大きな意味を持つ。

IoT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たい

SUIT,RATS,TEEP,MUD



IETF109オンライン（2020年11月開催）での TEEP(TEE Provisioning)に関する活動

- 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

TEEP Hackathonでは、日本から積極的に参加があった

第３回 鍵管理勉強会（オンライン開催）

JNSA主催セミナー一覧へ>>

■ 日　時：　2020年10月13日（火）14時00分～17時00分（13時45分からオンライン会場へ参加可能です）

■ 場　所：　オンライン会場（ Zoom ）

■ 参加費：　無料

■ 登　録：　登録サイト（Zoom事前登録制，定員200名）※受付は終了しました。

■ 世話役：　松本 泰氏 （JNSA 標準化部会PKI相互運用技術ワーキンググループリーダー／セコム株式会社IS研究所）

■ 講演資料　2020年10月15日掲載

【講演1】「暗号鍵管理の重要性」　松本 泰 氏　(8.9MB)
【講演2】「暗号鍵管理システム設計指針（基本編）概要」　神田 雅透 氏　(1.9MB)
【講演3】「暗号鍵管理に必要な仕組み」　伊藤 忠彦 氏　(4.6MB)
【講演4】「暗号鍵管理のためのHSM（仮題）」　舟木 康浩 氏　(3.8MB)
【パネルディスカッション】 「様々なシステムにおけるセキュリティの要となる暗号鍵管理」 ※後日公開予定

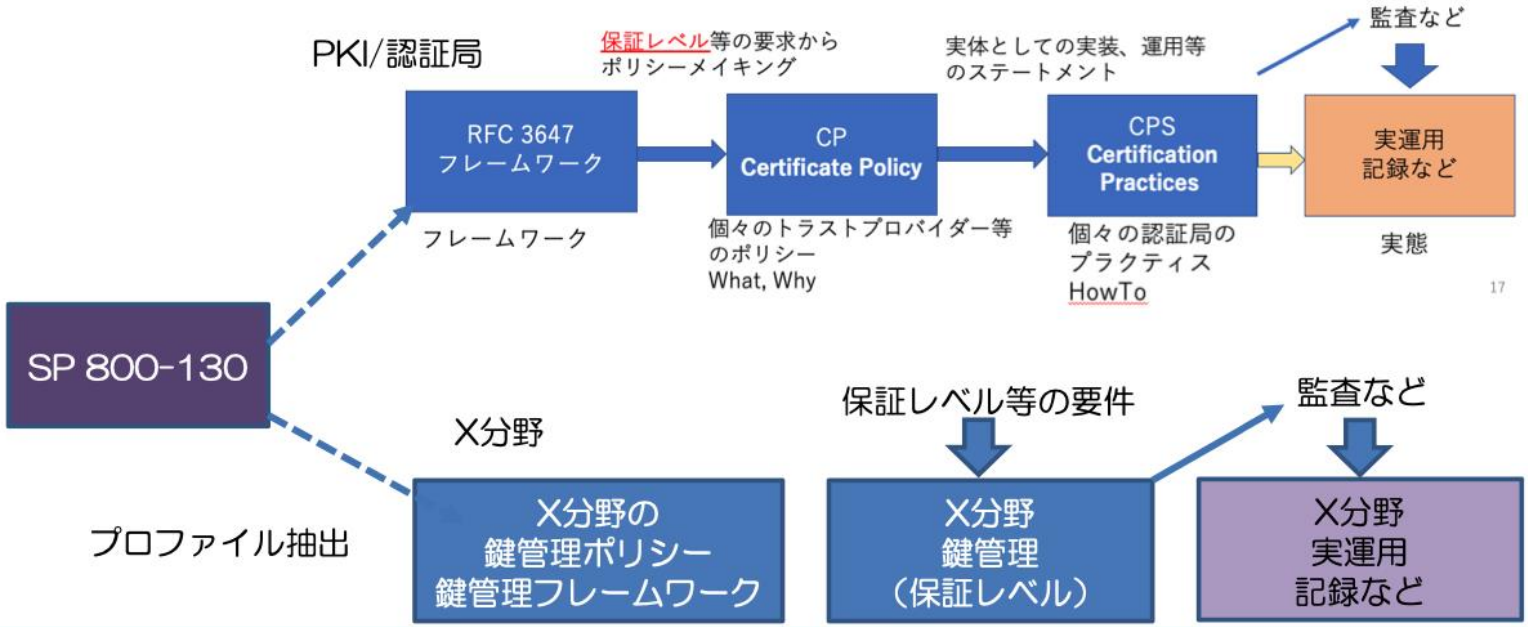
【開催趣旨】

自動車、暗号資産システム等の様々な分野のシステムに暗号技術が組み込まれ／利用されると同時に、様々なシステムの至る所に「暗号鍵」が組み込まれるようになってきました。この際、暗号鍵管理は、これらのシステムのセキュリティの要となります。しかし、この暗号鍵管理がどのように設計され運用されるべきか、なかなか分かりづらいところがあるのではないでしょうか。こうしたことを背景に2020年7月7日に、CRYPTREC/IPAから暗号鍵管理ガイドラインが公開されました。本勉強会では、この暗号鍵管理ガイドラインを中心に、暗号鍵管理のあるべき姿、設計の方法論、実装のあり方などを議論します。

出典：
第３回 鍵管理勉強会（オンライン開催）
https://www.jnsa.org/seminar/seckey/201013/index.html

SP 800-130　2013年

A Framework for Designing Cryptographic Key Management Systems



出典　：　暗号鍵管理の重要：https://www.jnsa.org/seminar/seckey/201013/data/1_matsumoto.pdf