信頼される安心を、社会へ。
SECOM

セキュアコンポーネントとPKIが作るデジタルトラストの世界
-- IETFのIoT標準化動向などから見えてくるIoTのプラットフォーム化 --

2021年9月27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）

JNSA 特定非営利活動法人 日本ネットワークセキュリティ協会 Japan Network Security Association

松本の自己紹介　セコム（株）IS研究所　ディビジョンマネージャー

信頼される安心を、社会へ。
SECOM

- 1984年　UNIX上のビデオテックス・パソコン通信システムの開発に従事
- 1994年　各種インターネットサービスの設計、開発、運用に従事
- 1999年　サイバーセキュリティ事業の立ち上げに従事
- 2003年-2007年　工学院大学「セキュアシステム設計技術者の育成」プログラム客員教授
- 2007年　経済産業省 商務情報政策局長表彰「情報セキュリティ促進部門」受賞
- 2007年-2012年　IPA 情報処理推進機構 情報セキュリティ分析ラボラトリー 非常勤研究員
- 2011年-2012年
  - 社会保障・税に関わる番号制度　情報連携基盤技術WG　構成員
  - 社会保障・税に関わる番号制度　社会保障分野サブWG　構成員
- 2013年-2014年
  - 内閣官房　パーソナルデータに関する検討委員会・技術検討WG　構成員
- 2008年-2018年　JDCC 日本データセンター協会　セキュリティWGリーダ
- 2021年9月現在
  - CRYPTREC 暗号技術検討会構成員、暗号技術評価委員会　委員、暗号技術活用委員会　委員
  - 日本ネットワークセキュリティ協会　標準化部会　副部会長
  - 日本ネットワークセキュリティ協会　PKI相互運用技術WGリーダ
  - 日本トラストテクノロジー協議会（2017年11月設立）副代表
  - JST/RISTEX 公私領域アドバイザー
  - QST SIP光・量子技術評価委員会委員
  - 津田塾大学総合政策学部非常勤講師（情報セキュリティ論）

セキュアコンポーネントとPKIが作るデジタルトラストの世界
-- IETFのIoT標準化動向などから見えてくるIoTのプラットフォーム化 --

信頼される安心を、社会へ。
SECOM

- セキュアコンポーネント（セキュリティチップ＋TEEなど）が組み込まれた膨大な数のIoTデバイスが、フィジカル空間に配置されつつあります。
  - → スケールアウトへの要求、プラットフォーム化している大きな理由
- この際、フィジカル空間に配置されるセキュアコンポーネントを内包したIoTデバイスとサイバー空間上のサービス間には、トラストが必要になりますが、ここにPKIが重要な役割を果たします。
- このような「セキュアコンポーネントとPKI」が提供するトラストは、サイバーフィジカルシステム（CPS）に大きな価値を提供します。
  - → デジタルトラストの世界
- 本講演では、IETFなどのIoT標準化など動向を中心に、デジタル社会を支える「セキュアコンポーネント ＋ PKI」の動向を説明します。

JNSA
特定非営利活動法人
日本ネットワークセキュリティ協会
Japan Network Security Association

本日のDPF研究会「企画主旨」との関係

信頼される安心を、社会へ。
SECOM

- DPF研究会において、ICカードやSIMから埋め込み型のeSIM(embedded SIM）、さらにはデバイスの高信頼実行環境TEE(Trusted Execution Environment）など、現在IoTデバイス・環境への搭載の議論が進展しつつあるセキュアコンポーネント技術に関して、GlobalPlatformなどの標準化動向を中心に政策・技術・導入展開など
- セキュアコンポーネント＆PKIなどクレデンシャルの役割 → 何かを証明したい
  - ICカード：人が所持することにより、人の証明（人の識別、属性の証明）など
  - SIM：モバイルデバイスに装着することによる携帯キャリアとの契約の証明
  - eSIM(embedded SIM：モバイルデバイスに組み込まれ、プログラマブルな携帯キャリアとの契約の証明
  - 高信頼実行環境TEE(Trusted Execution Environment）など、現在IoTデバイス・環境への搭載　→　ここが、本講演の主旨するところ
    - 従来からの「デバイスの識別・認証」
    - 様々なIoTデバイスの様々な信頼性（trustworthiness）の実行時の証明
    - → この部分が、クラウドサービスと連携して「プラットフォーム化」

セキュアコンポーネントとPKIが作るデジタルトラストの世界
-- IETFのIoT標準化動向などから見えてくるIoTのプラットフォーム化 --

- JNSA(日本ネットワークセキュリティ協会）PKI相互運用技術WGにおける活動
- IETFにおけるIoTセキュリティの標準化動向
  - IoTをスケーラブルに展開するIoTオンボーディング
- リモートアテステーション
  - 様々なIoTデバイスの様々な信頼性（trustworthiness）の実行時の証明
- デジタルトラストの目指す社会
- まとめ

日本ネットワークセキュリティ協会
PKI相互運用技術WGにおける活動

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

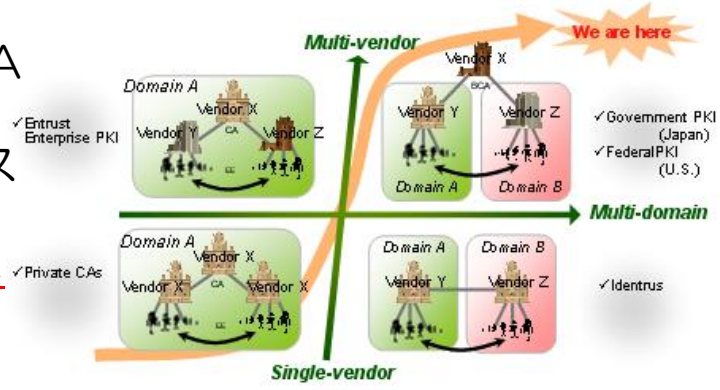
What's new?

- 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プロジェクト」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 & TRUST Days online 2021までの歩み

開催年	テーマ
2006	PKIの展開と最新技術動向
2007	PKIの展開と最新技術動向
2008	ＰＫＩの標準から実装まで最新動向
2009	様々な分野に展開されるPKIの最新動向
2010	社会基盤としてのPKI／PKIの10年
2011	番号制度時代のPKI
2012	我が国における信頼基盤の連携に向けて
2014	デジタル社会のための電子署名を見直す
2015	サイバーセキュリティの要となるPKIを見直す
2016	マイナンバー時代のPKI
2017	IoT・ブロックチェーン時代のPKI
2018	超スマート社会（Society 5.0）におけるトラストの在り方
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
2021	2021年4月15日（木）　テーマ：変貌するトラストアーキテクチャ 2021年4月16日（金）　テーマ：デジタルトラストにおける法と技術のあり方

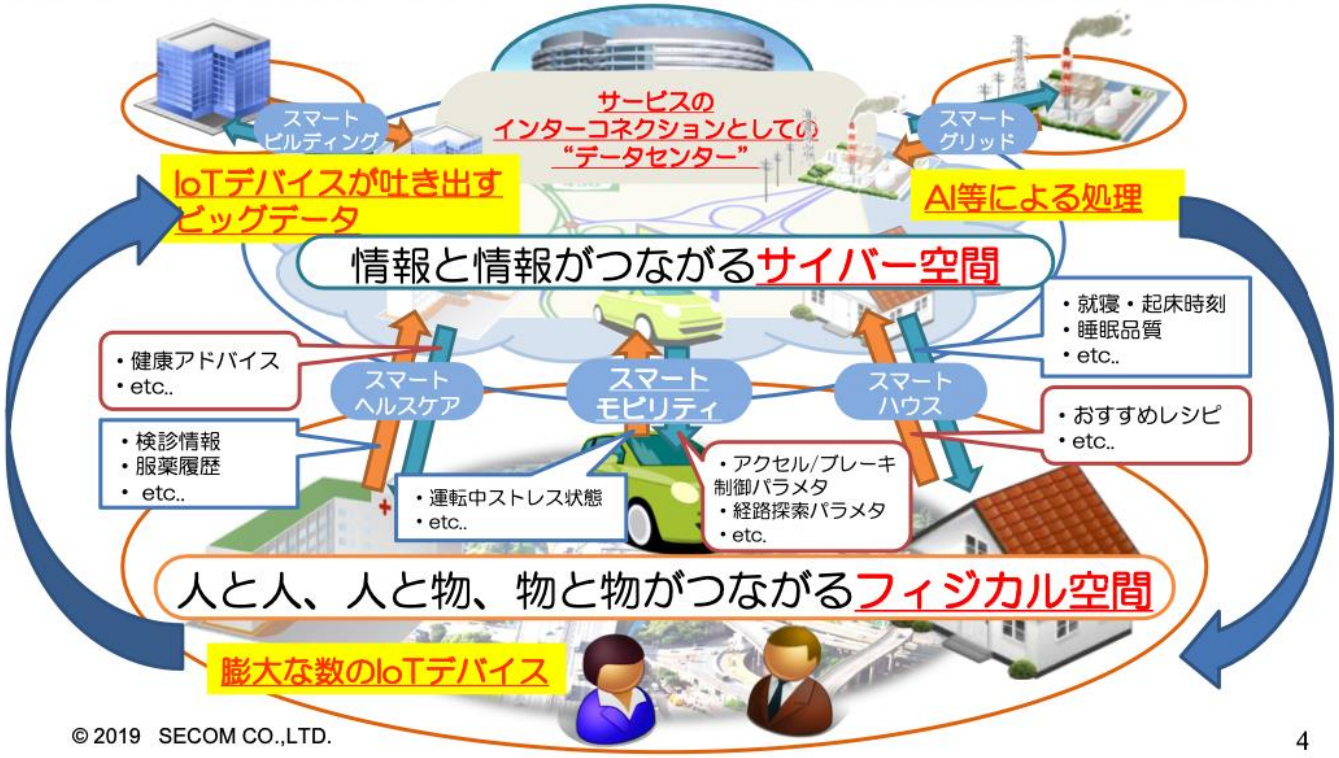
2017年頃からCPS（Cyber Physical Systems）におけるトラスト確立に向けたIETF等の標準化動向に注目

セコム IS研究所 Intelligent Systems Laboratory

信頼される安心を、社会へ。 SECOM

午前中の部　IoTのトラスト

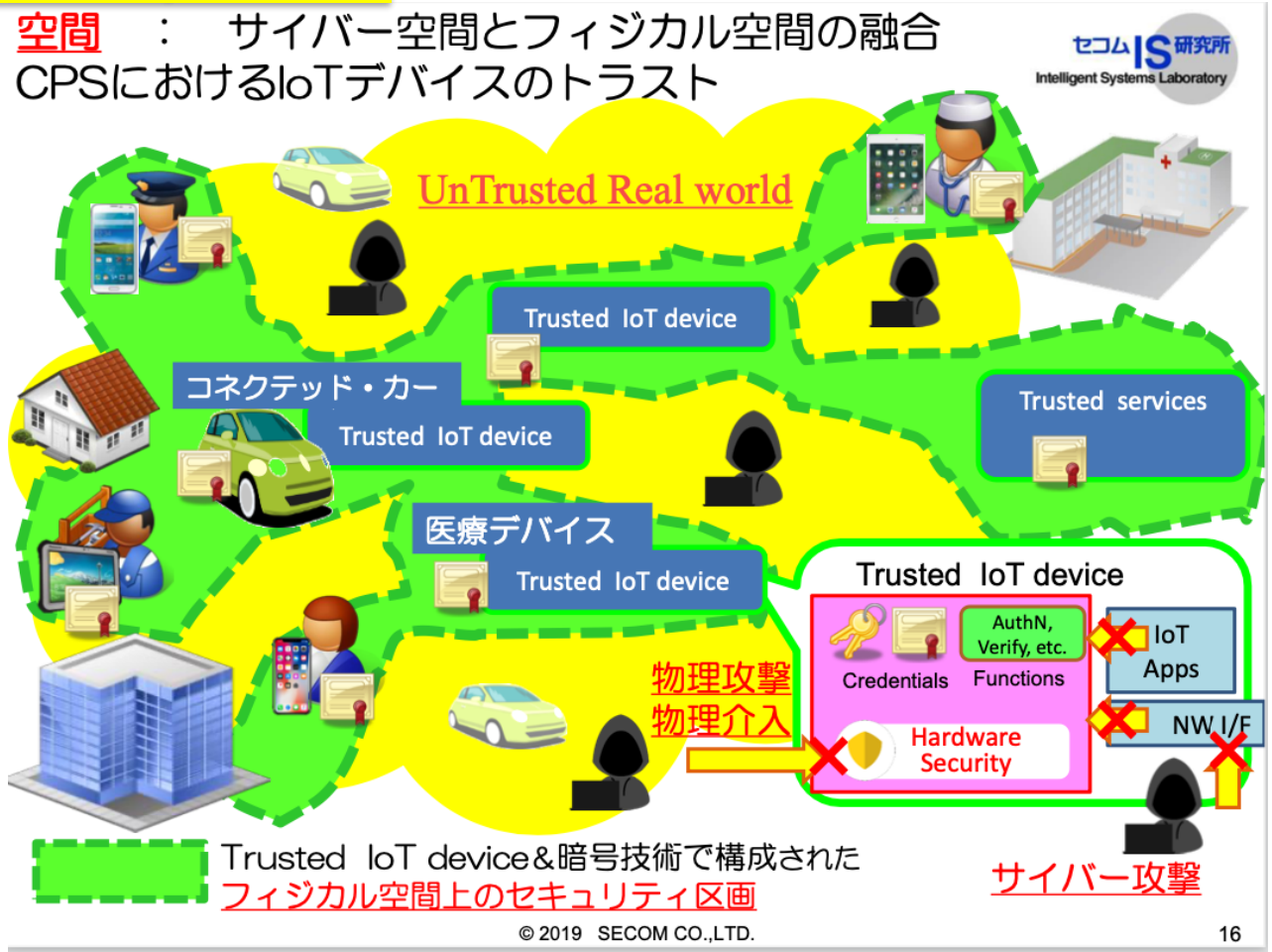
IoTサービスシステム ≒　CPS（Cyber Physical Systems）



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

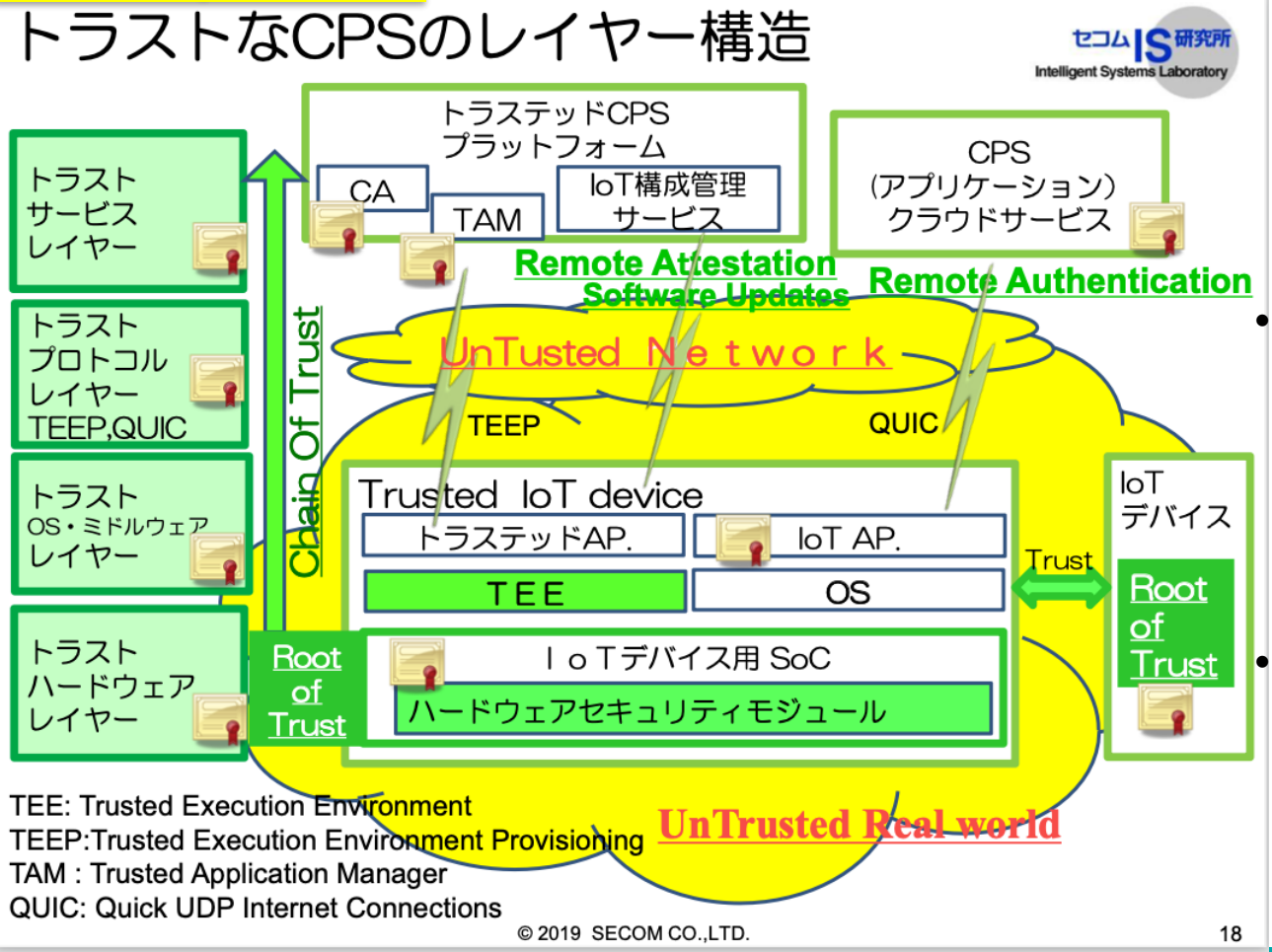


出典：
PKI Day 2019
2019年4月17日
https://www.jnsa.org/seminar/pki-day/2019/data/190417_am05_matsumoto.pdf

Trusted IoT devices（trusted smart 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必要。

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必要。

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。

PKI & TRUST Days online 2021　第1日目：2021年4月15日（木）
テーマ：変貌するトラストアーキテクチャ
https://www.jnsa.org/seminar/pki-day/2021/index.html#day1

信頼される安心を、社会へ。
SECOM

デジタルトラストアーキテクチャの要素技術をベースにトラストが構築されつつある
ゼロトラストネットワークとConfidential Computing

プラットフォームに組み込まれて行くセキュアコンポーネント

講演２
デジタルトラストとゼロトラストネットワーク
鈴木 研吾 氏（株式会社 LayerX シニアセキュリティアーキテクト

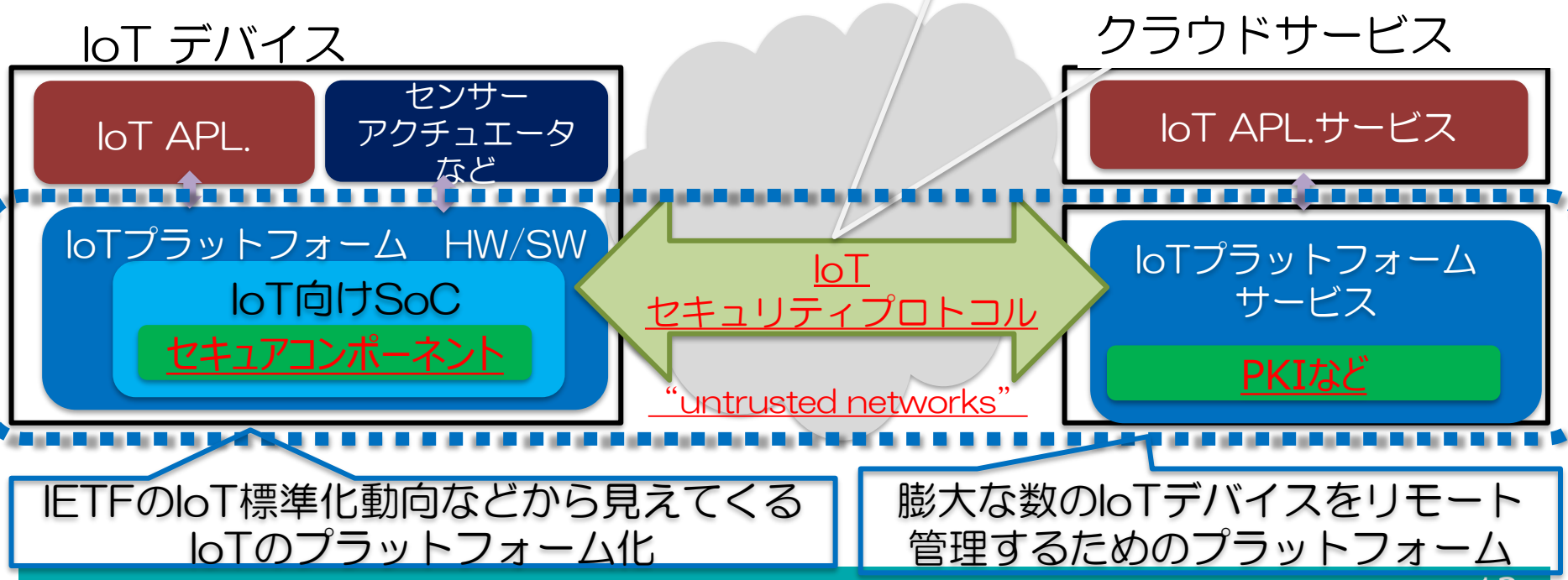
講演３
Confidential Computing の技術動向
奥田 哲矢 氏（NTTセキュアプラットフォーム研究所 研究主任）

講演４
プラットフォームで実装されるトラスト
プラットフォームに組み込まれて行くデジタルトラストアーキテクチャ
垣内 由梨香 氏
（Microsoft Corporation セキュリティ レスポンスチーム セキュリティ プログラム マネージャー）

講演１　トラストを確立する技術の概要
HW Root OF Trust
セキュアーブート
セキュアエンクレーブ・TEE
リモートアテステーション
セキュアコンポーネントの進化
宮澤 慎一 氏（セコム株式会社 IS研究所 主務研究員）

「デジタルトラストに対応するコンピュータアーキテクチャの変化」
コンピュータアーキテクチャ自体に暗号技術（主に公開鍵暗号技術）が取り込まれて行く
→　デジタル・トラストアーキテクチャ

IETFにおけるIoTセキュリティの標準化動向



IETFにおけるPKI関連の標準化活動

From: draft-shimaoka-multidomain-pki-13 — Informational
Network Working Group — M. Shimaoka, Ed. SECOM
Request for Comments: 5217 — N. Hastings NIST
Category: Informational — R. Nielsen Booz Allen Hamilton
July 2008

Memorandum for Multi-Domain Public Key Infrastructure Interoperability

Status of This Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Abstract

The objective of this document is to establish a terminology framework and to suggest the operational requirements of Public Key Infrastructure (PKI) domain for interoperability of multi-domain Public Key Infrastructure, where each PKI domain is operated under a distinct policy. This document describes the relationships between Certification Authorities (CAs), provides the definition and requirements for PKI domains, and discusses typical models of multi-domain PKI.

https://datatracker.ietf.org/doc/html/rfc5217

Internet Engineering Task Force (IETF) — T. Ito
Request for Comments: 8813 — SECOM CO., LTD.
Updates: 5480 — S. Turner
Category: Standards Track — sn3rd
ISSN: 2070-1721 — August 2020

Clarifications for Elliptic Curve Cryptography Subject Public Key Information

Abstract

This document updates RFC 5480 to specify semantics for the keyEncipherment and dataEncipherment key usage bits when used in certificates that support Elliptic Curve Cryptography.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8813.

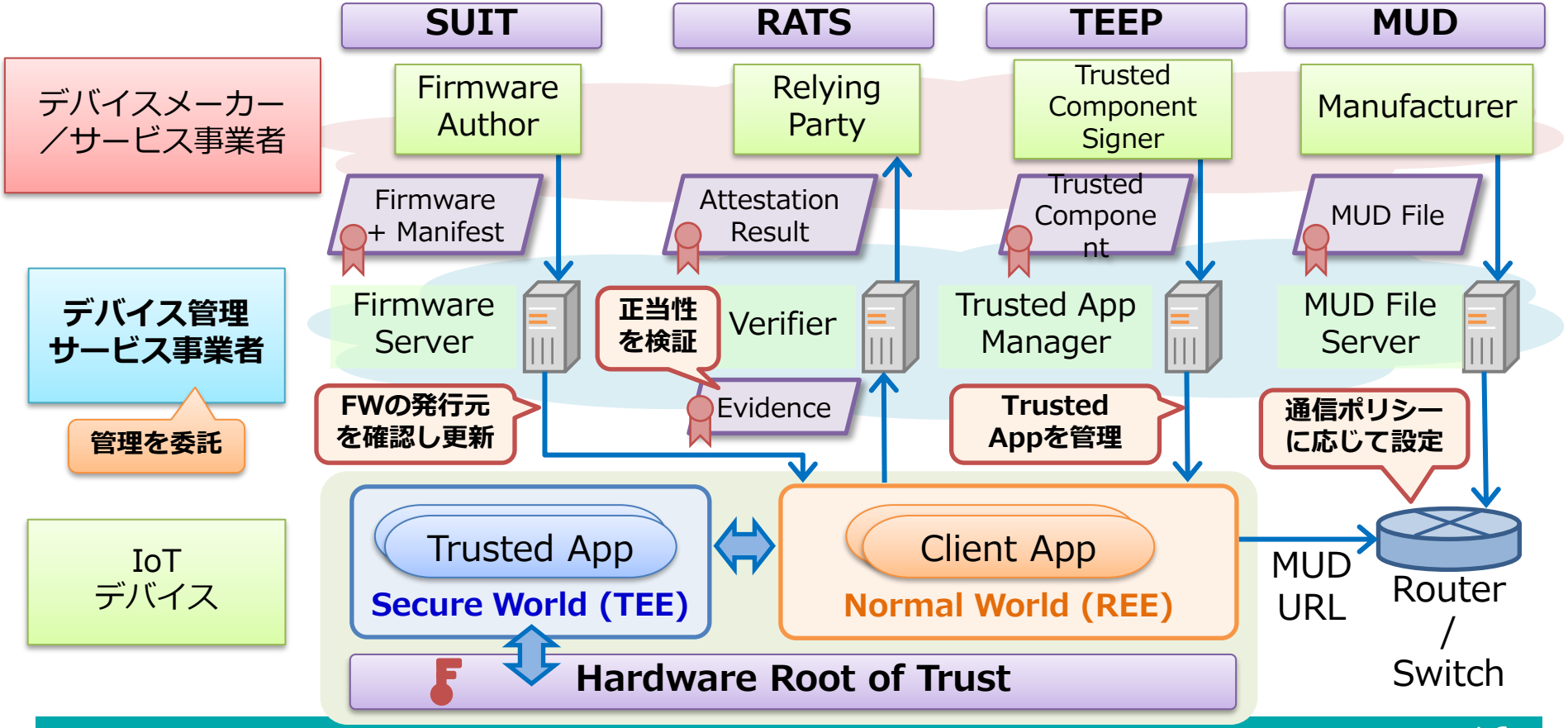
https://datatracker.ietf.org/doc/html/rfc8813

IETFにおけるIoTセキュリティの標準化動向
IETFにおけるIoTセキュリティプロトコルレイヤーの活動

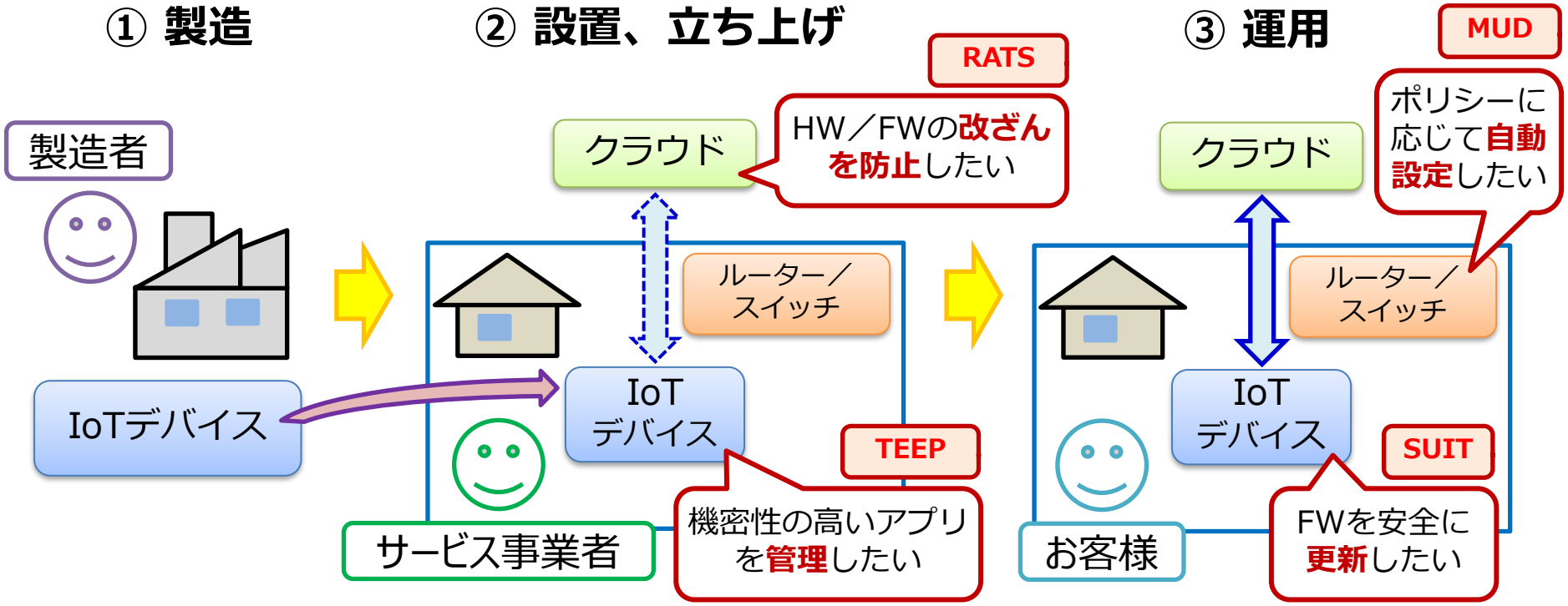
- SUIT　　Software Updates for IoT
  - https://datatracker.ietf.org/wg/suit/about/
- RATS　　Remote ATtestation ProcedureS
  - https://datatracker.ietf.org/wg/rats/about/
- TEEP　　Trusted Execution Environment Provisioning
  - https://datatracker.ietf.org/wg/teep/about/
- MUD　　Manufacturer Usage Description 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、ネッ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。これらのデジタル署名よりIoTデバイスとサービス間のトラストが確立する。
デジタル署名はセキュアコンポーネントにより保護された暗号鍵で署名され検証される

マルチステークホルダーで構築されるサイバーフィジカルシステム
セキュアコンポーネントを前提とした標準化

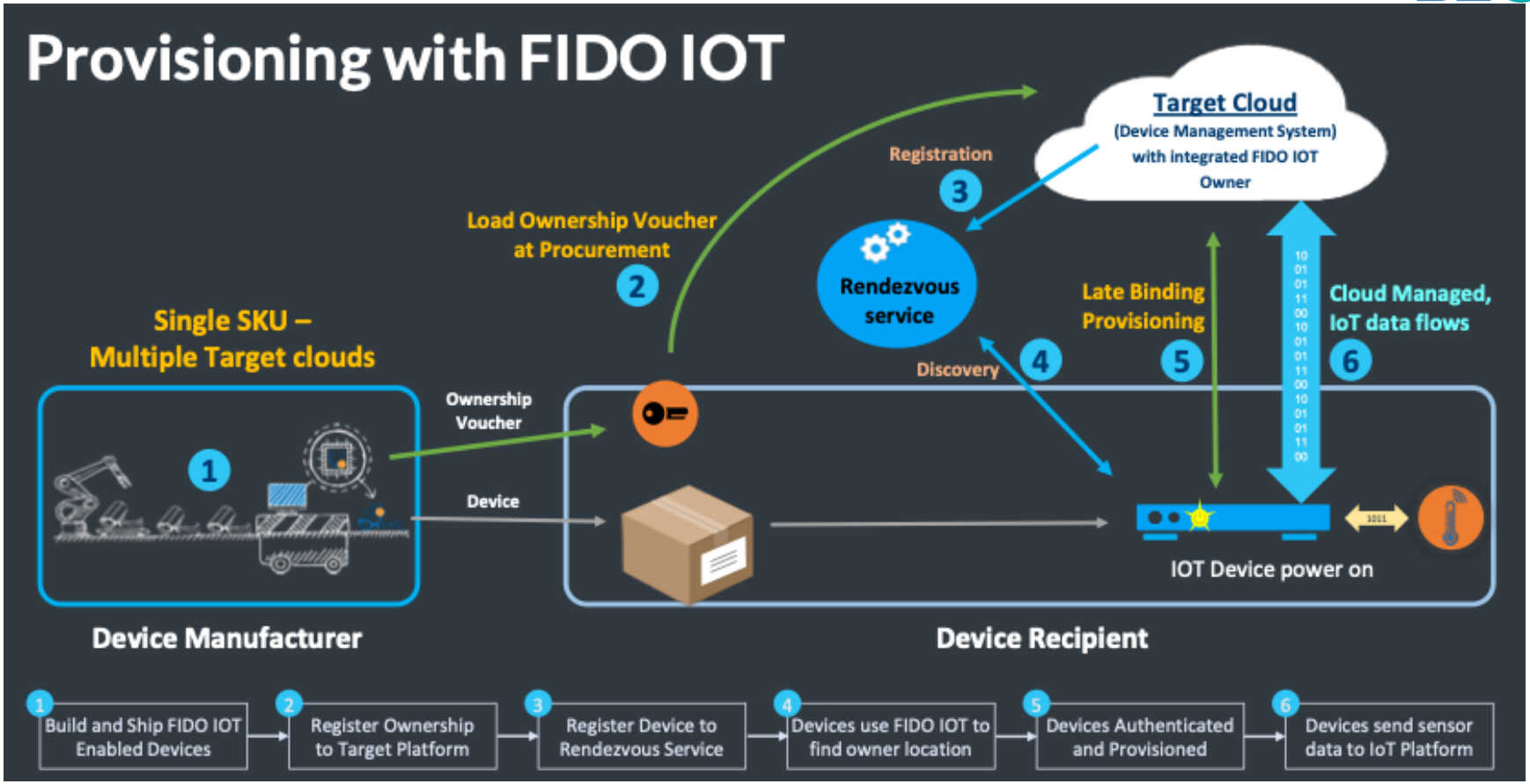


膨大な数のIoTデバイスをフィジカル空間に配置・展開・保守運用
→ スケールアウトへの要求、プラットフォーム化
そのための IoT onboarding を目指した標準化



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

IETF110（2021年3月開催） IOT Operations (iotops) WG



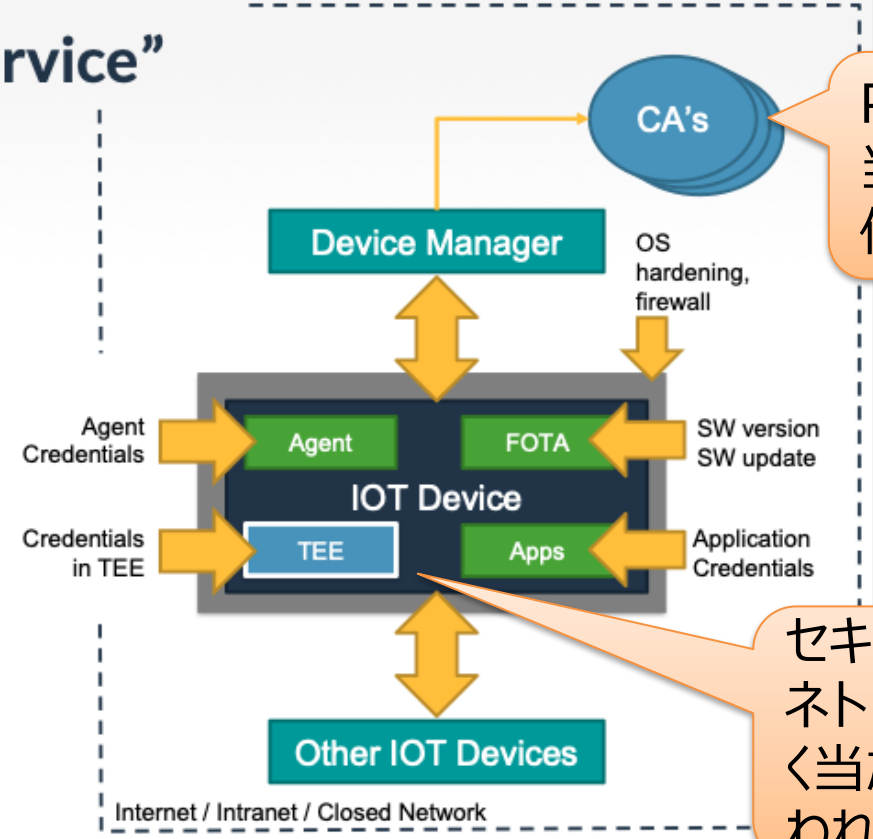
https://datatracker.ietf.org/meeting/110/materials/slides-110-iotops-fido-device-onboard-00

信頼される安心を、社会へ。
SECOM

FDO: Out of Box ➔ “in Service”

FDO Download:
- Initialization/Hardening Scripts including Agent
- Crypto and other Credentials
- Trust for local keys (CSR/Cert, multiple CA’s)
- Data files / programs (small, agent is most likely)

Use FDO to set up:
- Agents
- Software update (existing FOTA)
- Connection to other IOT devices
- FDO “Owner” to IOT devices
- Keys in TEE (e.g., using CSR)
- Devices in closed networks



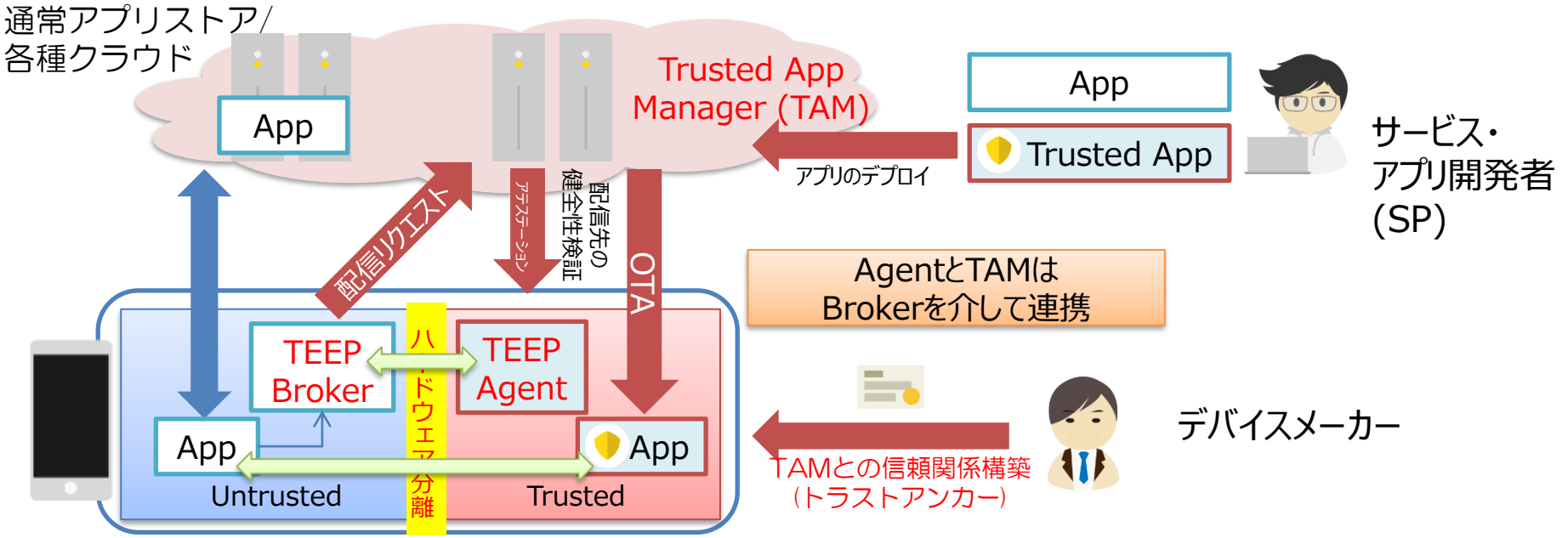
PKIが、ごく当たり前に使われる

セキュアコンポーネント・TEEが、ごく当たり前に使われる

https://datatracker.ietf.org/meeting/110/materials/slides-110-iotops-fido-device-onboard-00

TEEP(TEE Provisioning)

- TEE側で実行されるアプリの配信・管理の標準化を目指す
  - サービスの追加に合わせて決済や暗号化等の重要なアプリを追加/更新できるようにしたい



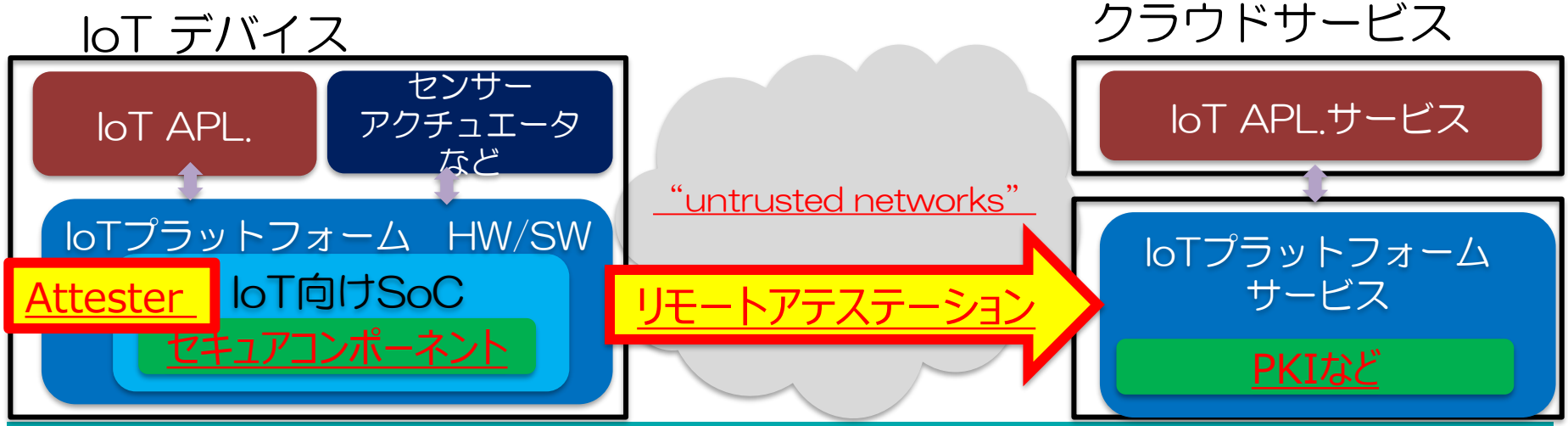
IETF109オンライン（2020年11月開催）での TEEP(TEE Provisioning)に関する活動

- 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(Trusted App Manager) 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

リモートアテステーション

IETF Remote ATtestation ProcedureS (rats)WG

高信頼実行環境TEE(Trusted Execution Environment）など、現在IoTデバイス・環境への搭載　→　ここが、本講演の主旨するところ
- 従来からの「デバイスの識別・認証」
- 様々なIoTデバイスの様々な信頼性（trustworthiness）の実行時の証明



リモート認証(Authentication)ではなくリモートアテステーションの要求
リモートのターゲットが「意図通り」動いているのか？

- On the Internet, Nobody Knows You're a Dog
- 「インターネットでは、実はキミが犬だって事を誰も知らないのさ」
- 1993年7月5日　米国の雑誌『The New Yorker』

２０２１年現在の課題
あんた（TP:Trusted Party）が犬でないことは分かったし、あんたが、私（RP: Relying Party）が信頼しているAさんであることも分かった。
けど、あんたのスマフォ（TP）は、大丈夫なの。乗っ取られているよみたいよ。

出典　https://en.wikipedia.org/wiki/On_the_Internet,_nobody_knows_you%27re_a_dog

IETF rats WG. Remote Attestation Procedures Architecture

https://datatracker.ietf.org/doc/draft-ietf-rats-architecture

2章. レファレンス・ユースケース. -- 7つのユースケース

今風のユースケース（デジタル社会的）

- 2.1. ネットワークエンドポイントアセスメント(Network Endpoint Assessment)
  - Attester ゼロトラスネットワークにおけるエッジデバイスなど
  - RP リソース・トラストエンジン
- 2.2. 機械学習モデルの保護 → AIエッジにおける学習済み機械データの保護
- 2.3. 機密データ保護 → コンフィデンシャルコンピューティング
- 2.4. 重要インフラストラクチャ制御 → デジタルツイン・サイバーフィジカルシステム
- 2.5. TEEのプロビジョニング（ Trusted Execution Environment Provisioning)
  - IETF TEEP WG https://datatracker.ietf.org/wg/teep/about/

ここで活動中

- 2.6. ハードウェアウォッチドッグ
- 2.7. FIDO バイオメトリクス認証（ Biometric Authentication）
  - ローカル認証につかう認証デバイス（ Authenticator）の信頼性（Trustworthiness）をリモートへ伝える（アテステートする）。
    - Ex. iOS. 14. から組み込まれた WebAuthN
      - https://developer.apple.com/videos/play/wwdc2020/10670/

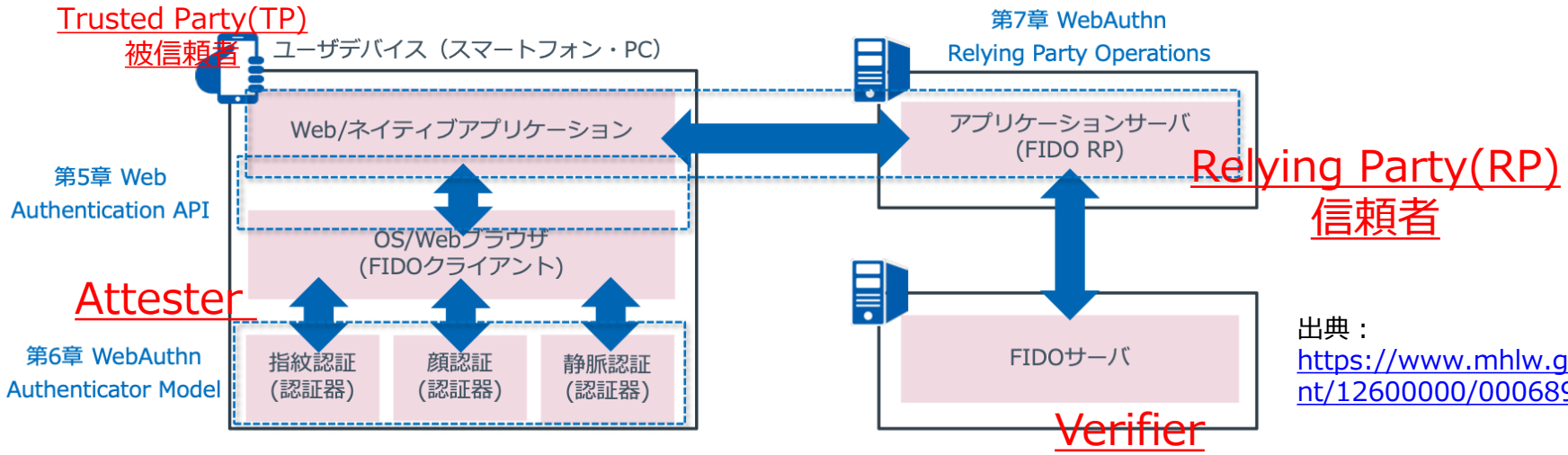
信頼される安心を、社会へ。
SECOM

WebAuthnではFIDOクライアントであるWebブラウザがサポートすべきAPI仕様を中心に記載されている。

ローカル認証に使用する認証デバイス（ Authenticator）の
信頼性（Trustworthiness）をリモートへ伝える（アテステート）

WebAuthn概要

- WebAuthnは2019年3月にWorld Wide Web Consortium(W3C)にて勧告された。
- WebAuthn仕様のうち主要項目として、FIDOクライアントがサポートすべきAPI(第5章)、認証器モデル(第6章)、RP(Relying Party、アプリケーション)側の操作(第7章)、Attestationのフォーマット仕様(第8章)が定められている。



出典：
https://www.mhlw.go.jp/content/12600000/000689751.pdf

Apple のWebAuthn. -- Apple のFIDO2対応実装

出典： Meet Face ID and Touch ID for the web
https://developer.apple.com/videos/play/wwdc2020/10670/

- 「Face ID and Touch ID」は、ローカル認証
- リモート認証のRPは、ローカル認証をトラスト出来るのか？

3分17秒

Fourth, authenticators can, if necessary, prove their properties cryptographically via a process called attestation.

４分52秒

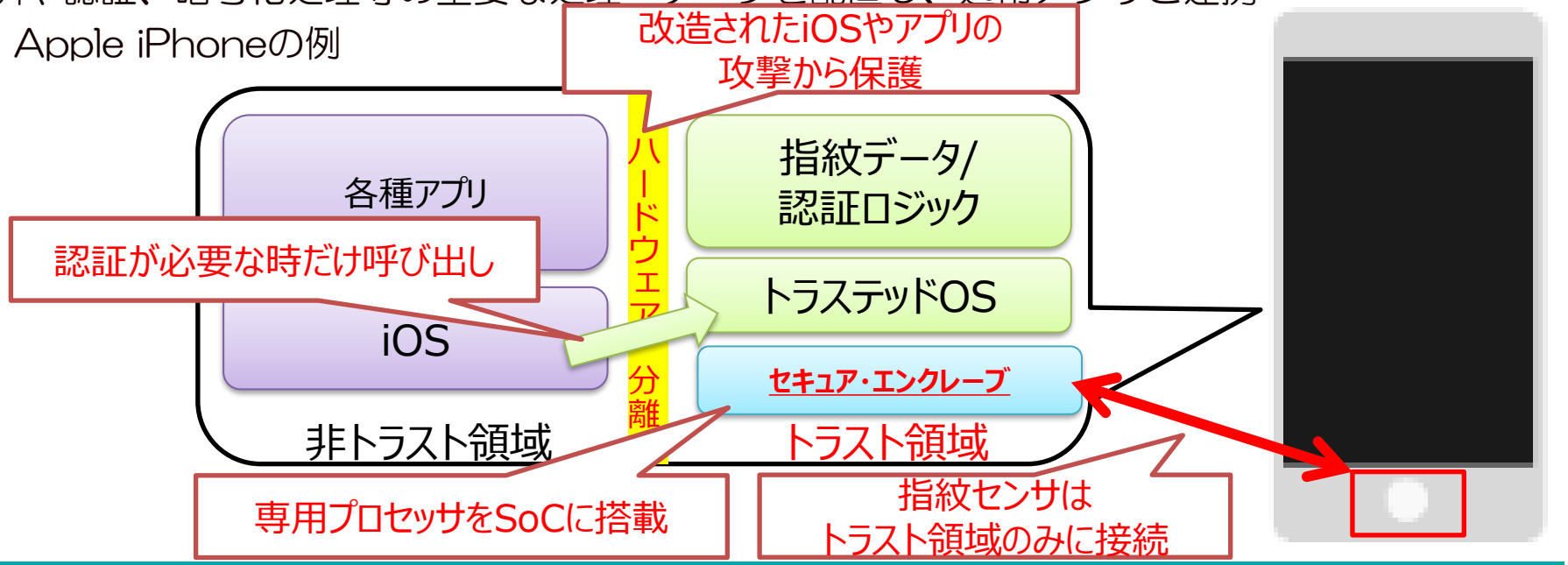
An authenticator like the iPhone is called a platform authenticator, because the authenticator is a feature built into the platform. There are two important properties that Apple builds into the authenticator. The first one, as we saw, is the Face ID and Touch ID, which is used to verify users' identity.
The second one is Secure Enclave, which is a processor that manages all the private keys and guarantees that they cannot leave the device.

「ハードウェアセキュリティと生体認証: Secure Enclave、専用のAES暗号化エンジン、Touch ID、Face IDなど、Appleデバイスのセキュリティの基盤をなすハードウェア」これの意味するところ

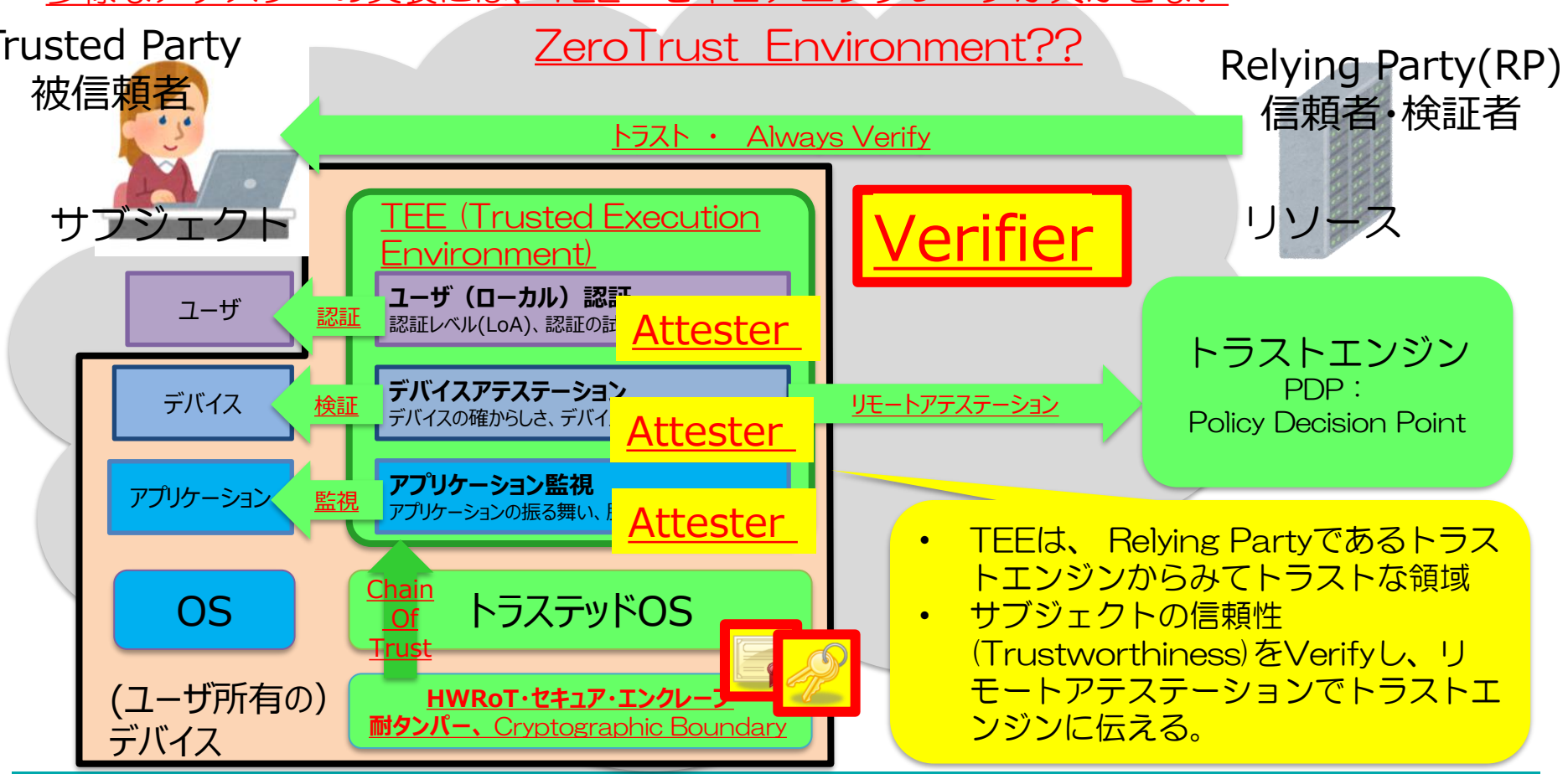
- ハードウェアにより通常アプリ,iOSと隔離されたトラスト領域（TEE（Trusted Execution Environment）
- トラスト領域：通常アプリやOSが改ざん等の侵害されても影響を受けない

決済や認証、暗号化処理等の重要な処理・データを配置し、通常アプリと連携

- Apple iPhoneの例



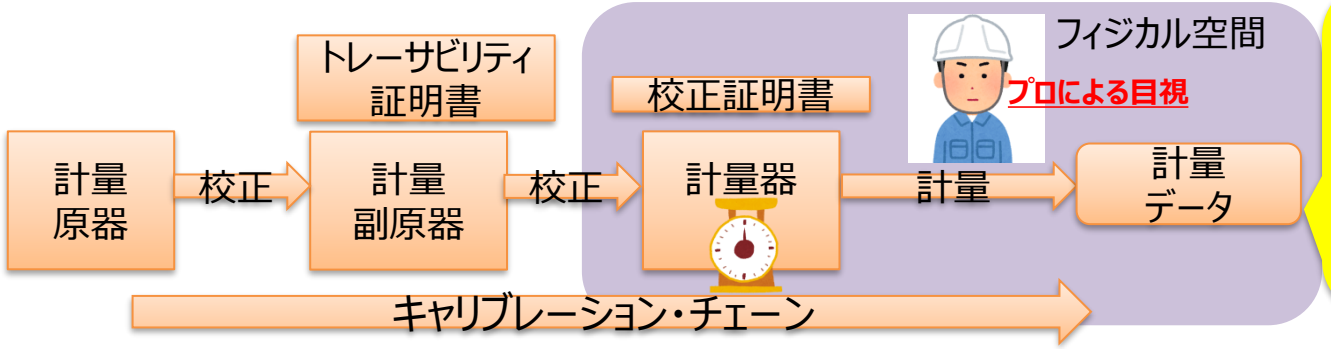
ゼロトラストネットワークではなく「ゼロトラスト環境のトラステッド・エッジ」
→ 多様なアテスターの実装には、TEE・セキュアエンクレーブが欠かせない



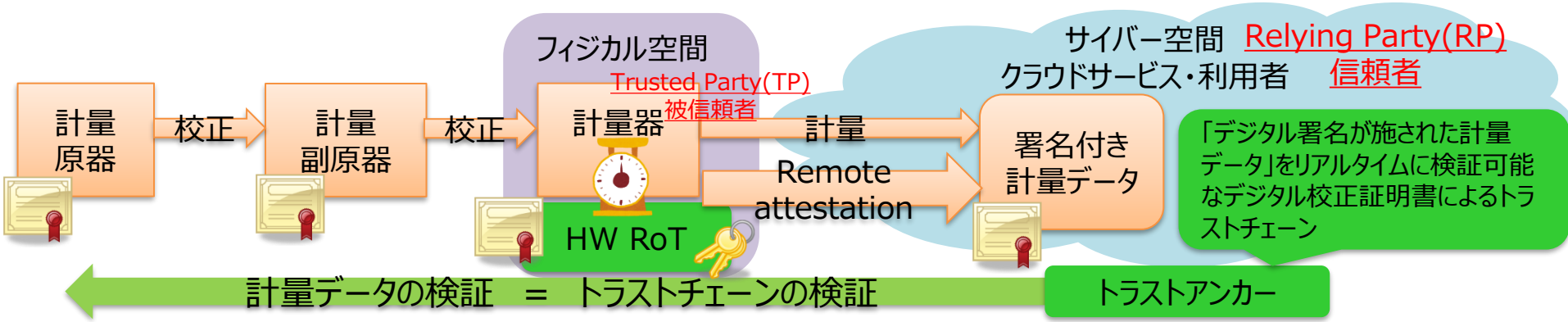
デジタルトラストが目指す社会

- セキュアコンポーネントとPKIが作るデジタルトラストの世界　→　何が実現できるのか？
- デバイスの信頼性（ Trustworthiness ）がリモートから暗号技術により検証可能になるデジタルトラストの世界

セキュアコンポーネントとPKIの役割　-- CPS上のトラスト
例えば、計量（計測）データの信頼性（Trustworthiness）では



計量（計測）データの信頼性（Trustworthiness）で最も重要なことは、計量器、計量データのキャリブレーション・チェーン が証明、保証されていること。



PKI・トラスト技術の役割　→　デバイス・データの信頼性（Trustworthiness）をRPに伝える
→ 人の目視に頼らず、デバイス・データの信頼性（Trustworthiness）が検証できること

Role of PKI / Trust Technology--Trust in Cyber-Physical Systems

信頼される安心を、社会へ。 SECOM

Trustworthiness as a medical device in physical space
Trustworthiness as an autonomous vehicle in physical space
Etc…

EU eIDAS
eSeal certificate

Singed

digital Certificate of Conformity

trust relationship

Trust anchor
eIDAS Trustt List

Physical space

Instrument
Trustworthiness

Trust

Cyberspace
Cloud service / user (trustee, RP)

trust relationship

GP

Chain Of Trust

TEEP Broker

TEEP Agent

Hardware isolation

App

App

Untrusted

Trusted

Singed data

Remote attestation

Signed data

Trustworthiness as an instrument in physical space

secure boot

secure storage

Secure MCU. HW RoT

Hardware security

trust relationship

Trust anchor

The role that PKI・Trust Technology should play

まとめ・結論？

セキュアコンポーネントとPKIが作るデジタルトラストの世界
-- IETFのIoT標準化動向などから見えてくるIoTのプラットフォーム化 --

プラットフォーム化の観点 → スケールアウトするIoTビジネス

IoTのスケールアウトを可能にする「セキュアコンポーネントとPKIが作るデジタルトラスト」

エンクレーブ・TEEなどが作り出すSocity5.0時代のトラスト スケールアウトするトラストへの要求??

- これまでのスケールアウト　　クラウドコンピューティング
  - 2005年出版GOOGLEクラウドの核心--巨大データセンターの変貌と運用の経済学
- スケールアウトするトラスト??　-> スケールアウトは、Socity5.0時代的要求？？
  - 膨大な数のデバイス、あらゆるもののConnect化、スマート化、これらのためのトラスト
  - コフィデンシャルコンピューティング（の経済学???）
    - HWRoot Of Trust・ Cryptographic Boundary をトラストの起点に、(PKIのような）暗号鍵の関係性で実現されるトラストモデルをベースに「 Trust Boundary」をスケーラブルに拡張する技術に思える。
  - トラステッドデバイス（トラステッドIoTデバイス）（の経済学???）
    - 既に膨大な数のスマートフォンに組み込まれている TEE(Trusted Execution Environment)
    - IoTデバイスへのセキュリティ要求が（プラットフォームセキュリティ）、そのまま（ファブレス）シリコンベンダーが設計するSoC(System-on-a-chip)へ
    - ＃超巨大印刷工場であるTSM＊が、ただひたすら輪転機を回す

参考スケールアウトするIoTデバイスのトラスト

出典：
PKI & TRUST Days online 2021「デジタル社会におけるトラスト」
変貌するトラストアーキテクチャ
https://www.jnsa.org/seminar/pki-day/2021/data/0415matsumoto.pdf

セキュアコンポーネントとPKIが作るデジタルトラストの世界
-- IETFのIoT標準化動向などから見えてくるIoTのプラットフォーム化 --

信頼される安心を、社会へ。
SECOM

- 従来、フィジカル空間で利用されているデバイスは、人が物理的に管理することを前提に、様々な信頼性（Trustworthiness）を維持、提供していた。
- “Untrusted real world” においても利用可能なセキュアコンポーネントとPKI が作り出すTrusted IoT deviceは、人手による物理的な管理なしに、リモートから管理のみで、信頼性（Trustworthiness）を提供するデバイスとなり得る。また、人の目視に頼らず、デバイス・データの信頼性の検証も可能となり得る。
- フィジカル空間に設置されたTrusted IoT deviceと、サイバー空間の間のトラストが確立は、フィジカル空間のサービスやビジネスを大きく変えていくと考えられる。
- このトラストの確立には、 Trusted IoT device に組み込まれたHW Root OF Trust等が組み込まれたセキュアコンポーネントと強く結びついたPKI等のトラスト技術が必要不可欠となる。
- society5.0時代のサイバーフィジカルシステムを念頭に置いた場合、多様なビジネス、サービス、マルチステークホルダーに対応したトラスト確立への要求（ ≒ PKI的要求）には、まだ、多くの課題がある。こうした課題解決が積極的に行われることを期待する。

参考リンク

- ゼロトラストにおけるトラスト（第25回サイバー犯罪に関する白浜シンポジウム テーマ）
  - 2021/5/21.　松本
  - https://sccs-jp.org/wp-content/uploads/2021/05/06y9c4q7th.pdf
- AI・IoT によるイノベーションを支える暗号技術によるトラスト
  - JNSA Press 第47号　2019年6月発行　　松本
  - https://www.jnsa.org/jnsapress/vol47/2_kikou-2.pdf
- PKI & TRUST Days online 2021　「デジタル社会におけるトラスト」
  - 第１日目：2021年4月15日（木）　テーマ：変貌するトラストアーキテクチャ
    第２日目：2021年4月16日（金）　テーマ：デジタルトラストにおける法と技術のあり方
  - https://www.jnsa.org/seminar/pki-day/2021/index.html
- 「トラストを確立する技術の概要 ～ どのような技術がなぜ作られてきたのか ～」　by　SECOM 宮澤氏
  - https://www.jnsa.org/seminar/pki-day/2021/data/0415miyazawa.pdf
- プラットフォーム セキュリティの技術の変遷　　（SCIS論文集） by SECOM 宮澤氏
  - https://www.iwsec.org/scis/2020/program.html
- スマートフォン等のスマート・デバイスに おけるセキュリティ:プラットフォーム化 によるリスクの現状と展望
  - https://www.imes.boj.or.jp/research/papers/japanese/20-J-17.pdf
- 第７回DPF研究会　Trustを巡る技術動向　~Confidential Computingを中心に~　　By　NTT 奥田哲也氏
  - https://www.ieice.org/~dpf/wp-content/uploads/2021/04/Trustを巡る技術動向_20210616_2.pdf

宣伝　2021年10月15日（金）開催
デジタルの日・JNSA標準化部会主催セミナー
「DXのためのデジタルトラスト実現に向けて」

- デジタルトランスフォーメーション（DX）実現のためには、紙文書や押印などに依存した既存の仕組み（既存のトラストのメカニズム）もまた、デジタルを前提としたトラストの仕組み（デジタルトラスト）に変革していく必要があります。
- また、セキュリティにおいてもこれまでの境界線防御によるセキュリティからゼロトラストへの大きな変革の潮流がありますが、これはデジタル庁が掲げるデジタル改革にも重要な意味を持つと考えられます。
- 本セミナーでは、トラストサービスなどの法制度、ゼロトラストを実現するためのアイデンティティ管理、これらのベースとなるプラットフォームで実装されるトラストなどDXのためのデジタルトラストの実現に向けたあり方を議論します。

参考

- サイバーフィジカルシステムにおけるトラスト
- 変貌するトラストアーキテクチャ
- IoTデバイス＆プラットフォームに組み込まれるトラストのメカニズム
- プラットフォームに実装されるトラスト：Appleの場合

サイバーフィジカルシステムにおけるトラスト
-- society5.0時代におけるデジタルトラスト --

- サイバーフィジカルシステムにおけるデジタルトラストのための利用されていくであろう TEE/Enclave

サイバーフィジカルシステム ≒ IoT ・BD・AI

信頼される安心を、社会へ。
SECOM

法と技術アーキテクチャ

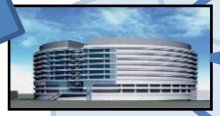
技術

技術アーキテクチャと
ビジネス・デザイン

法制度

AIなどによる処理

ビジネス



ビッグデータの収集

情報と情報がつながるサイバー空間

フィジカル空間に還元
新たな価値の創造

デジタル・ツイン

高機能なエッジAI

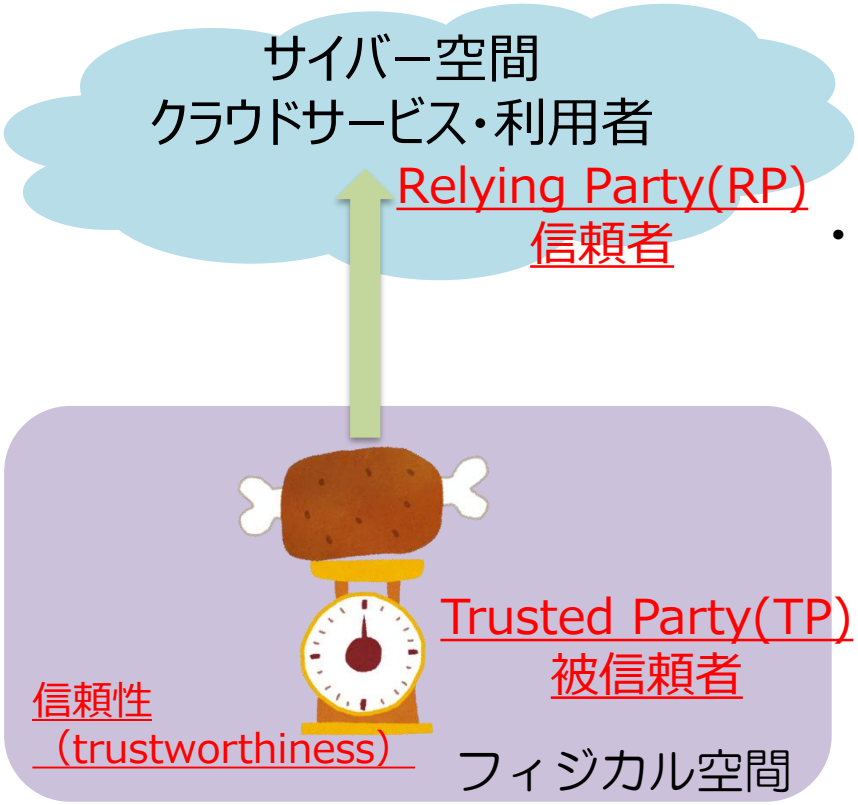
学習済
モデル

フィジカル空間における
サービスイノベーション

膨大な数のIoTデバイス

人と人、人とモノ、モノとモノがつながるフィジカル空間

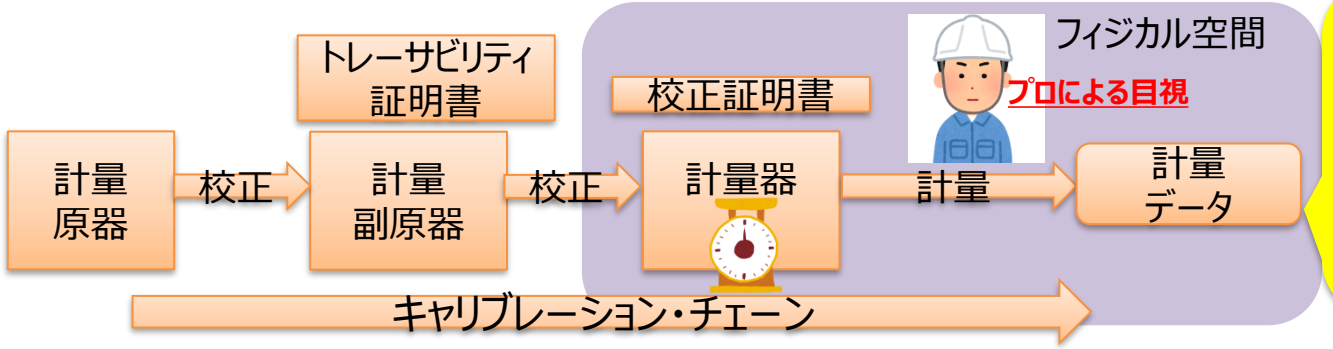
サイバーフィジカルシステムにおけるトラスト
フィジカル空間にある「はかり」をサイバー空間から利用するというシナリオ



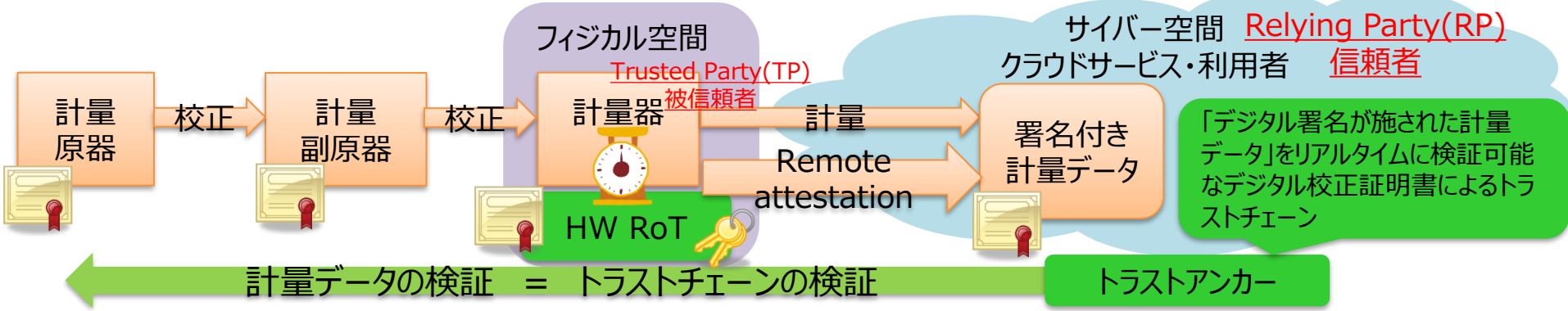
- 「測る」ということに関しては
  - クラウドサービスは、信頼者：Relying Party(RP)
  - はかりは、被信頼者：Trusted Party(TP)
- では被信頼者である「はかり」の信頼性（Trustworthiness）は？
  - クラウドサービスは、「はかり」の信頼性について何を知りたいのか？
  - リモート（クラウドサービス）に、重さを伝えるための「はかり」というIoTデバイスセキュリティも信頼性の一つの要素
  - しかし、はかりの信頼性としてクラウドサービス伝えらいことは？？？

PKI・トラスト技術の役割　-- サイバーフィジカルシステムにおけるトラスト

例えば、計量（計測）データの信頼性（Trustworthiness）では



計量（計測）データの信頼性（Trustworthiness）で最も重要なことは、計量器、計量データのキャリブレーション・チェーン が証明、保証されていること。



PKI・トラスト技術の役割　→　デバイス・データの信頼性（Trustworthiness）をRPに伝える
→ 人の目視に頼らず、デバイス・データの信頼性（Trustworthiness）が検証できること

Role of PKI / Trust Technology--Trust in Cyber-Physical Systems

信頼される安心を、社会へ。 SECOM

Trustworthiness as a medical device in physical space
Trustworthiness as an autonomous vehicle in physical space
Etc…

EU eIDAS
eSeal certificate

Singed

digital Certificate of Conformity

trust relationship

Trust anchor
eIDAS Trustt List

Physical space

Instrument
Trustworthiness

Trust

Cyberspace
Cloud service / user (trustee, RP)

trust relationship

Chain Of Trust

TEEP Broker

Hardware isolation

TEEP Agent

App

Untrusted

App

Trusted

Singed data

Remote attestation

Signed data

Trustworthiness as an instrument in physical space

secure boot

secure storage

Secure MCU. HW RoT

Hardware security

trust relationship

Trust anchor

The role that PKI・Trust Technology should play

規制に組み込まれるべきデジタルトラスト

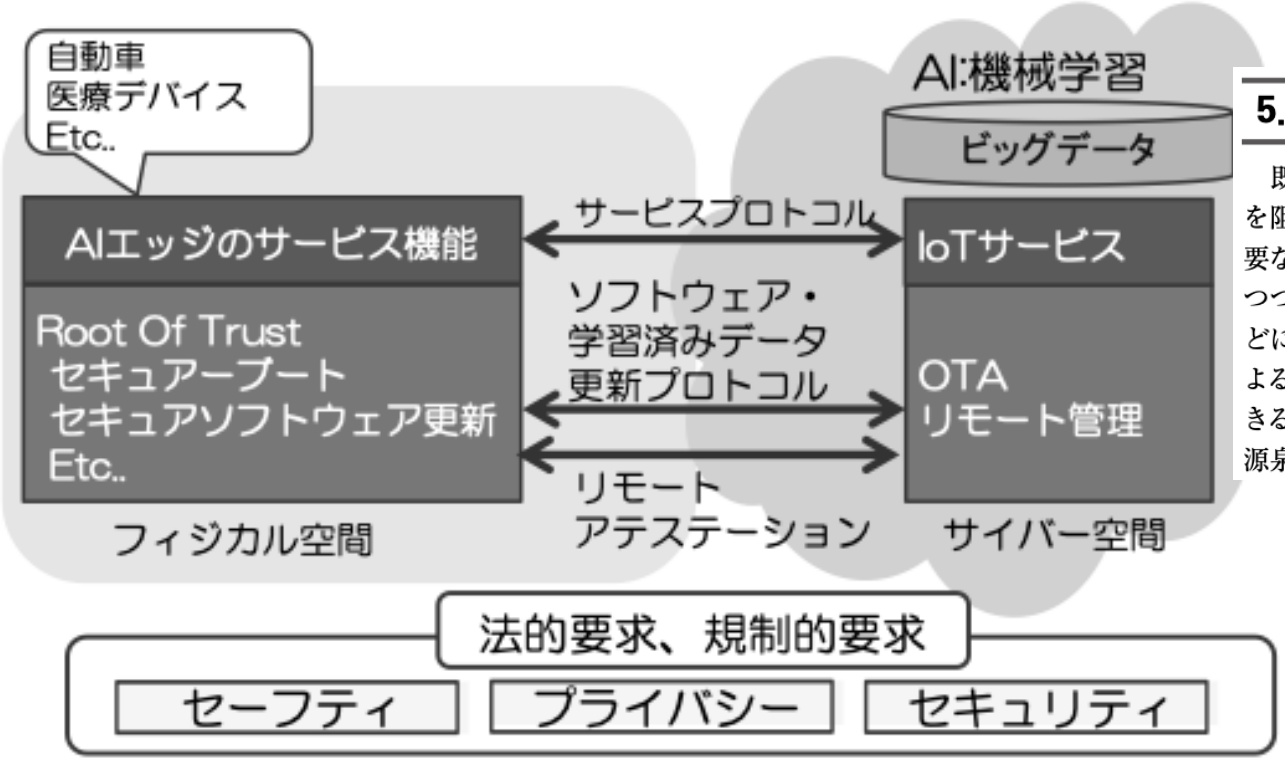


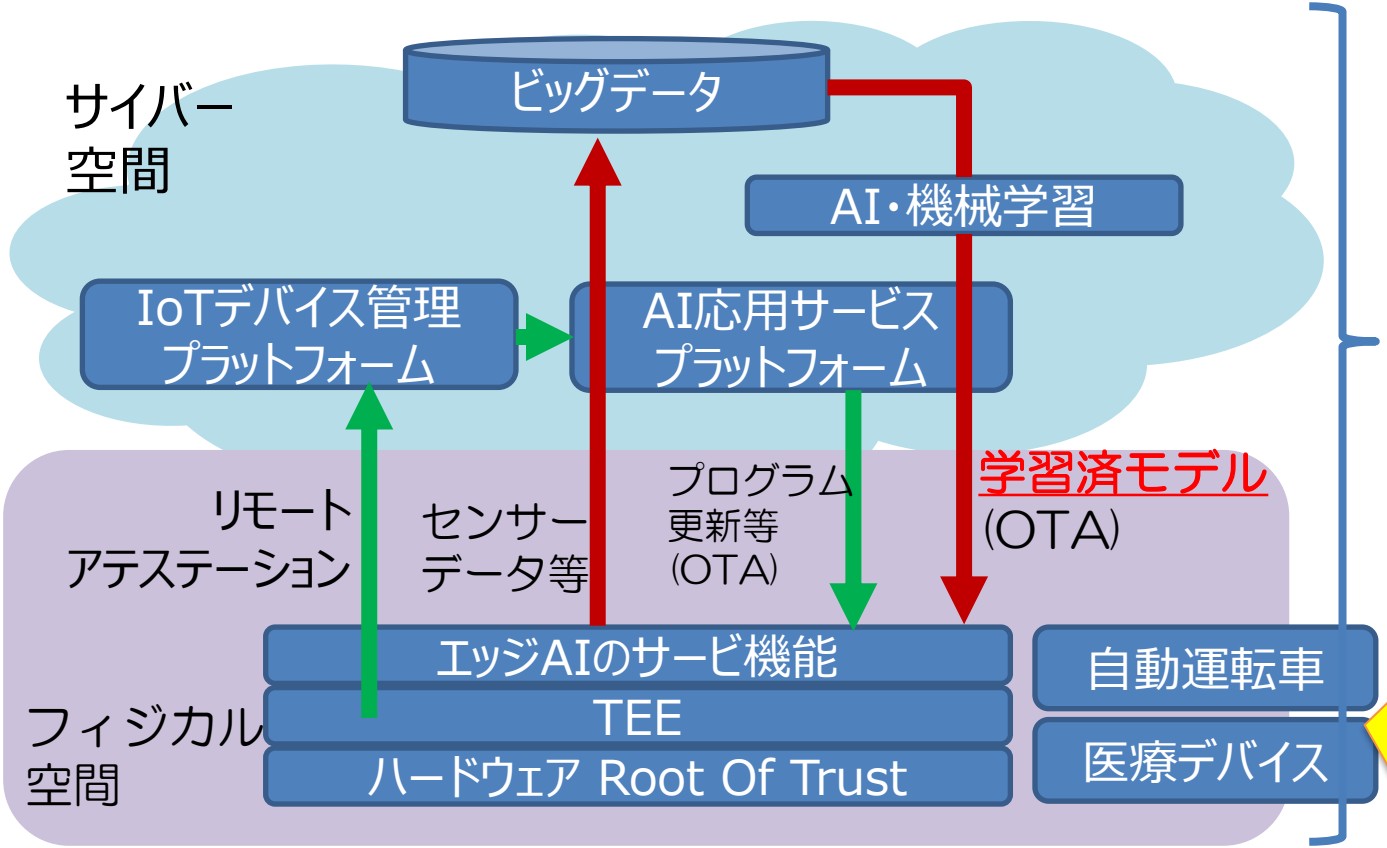
図1. AIエッジ、機械学習、規制の関係

5. おわりに

既存の法規制等が、AI・IoTによるイノベーションを阻害していると考えられる一方、本質的に規制が必要な分野においては、規制のパラダイムシフトが起こりつつある。こうした分野においては、新たな法規制などに対応できるIoTデバイス・AIエッジの暗号技術によるトラストが重要となり、これらが低コストで実現できることが、今後の超スマート社会における競争力の源泉ともなる。

出典： AI・IoTによるイノベーションを支える暗号技術
https://www.jnsa.org/jnsapress/vol47/2_kikou-2.pdf

サイバーフィジカルシステムにおけるトラスト技術
⇒　デジタルツイン・エッジAIを含むインテグリティ



- 膨大な数のIoTデバイス
- 高機能なエッジAI
- この循環に対するインテグリティがサイバーフィジカルシステムのトラストを支える

フィジカル空間における法的・規制的要求
- セーフティー
- プライバシー
- セキュリティ

トラスト・ビジネスデザイン的観点 – スケールアウト

信頼される安心を、社会へ。
SECOM

クラウドとIoTデバイスが持つ、暗号鍵とクレデンシャルにより強固なIoTのトラストを実現する。

クラウド

強固な物理セキュリティ環境のデータセンターにおけるトラストな運用

大量の（TEE&ハードウェアセキュリティを具備した）IoTデバイスをセキュアにクラウドからリモート管理
→ スケールアウトするプラットフォーマのビジネスモデル

クラウドからみてトラストな実行環境（TEE）

便利なIoTデバイスによるサービスを享受したいが、ネットワーク＆デバイスの管理はしたくない利用者

高機能なIoT ソフト

TEE

ハードウェアセキュリティ
HW Root of Trust

HOME

IoTデバイスからすると管理者不在で信頼できない環境（ゼロトラストネットワーク）

変貌するトラストアーキテクチャ
Root Of Trust、公開鍵暗号技術が組み込まれたSoC/CPUの世界

- CPU・SoCに組み込まれるトラスト(公開鍵暗号技術)
  - TEE(Trusted Execution Environment)という境界線防御で守られた場所
  - エンクレーブ(飛び地)というリング・プロテクションでは実現できない境界線　→　特権ユーザ問題も変えていく
- TEE・エンクレーブが実装されたSoCは、膨大な数が生産され、スマートフォン等に当たり前に実装され、デジタルトラストが形成しつつある？？
  - ex.公開鍵暗号技術が組み込まれたSoC/CPU CPU・SoCは、知らなくとも、これらが組み込まれた自分の持ち物であるはずのスマフォは、トラストしている（そうじゃないと生活できない）。

4月15日「変貌するトラストアーキテクチャー」４つの講演とキーワードとの関係

出典：https://www.jnsa.org/seminar/pki-day/2021/index.html

デジタルトラストアーキテクチャの要素技術をベースにトラストが構築されつつある
ゼロトラストネットワークとConfidential Computing

講演２
デジタルトラストとゼロトラストネットワーク
鈴木 研吾 氏（株式会社 LayerX シニアセキュリティアーキテクト）

講演３
Confidential Computing の技術動向
奥田 哲矢 氏（NTTセキュアプラットフォーム研究所 研究主任）

講演１　トラストを確立する技術の概要
HW Root OF Trust
セキュアーブート
セキュアエンクレーブ・TEE
リモートアテステーション
宮澤 慎一 氏（セコム株式会社 IS研究所 主務研究員）

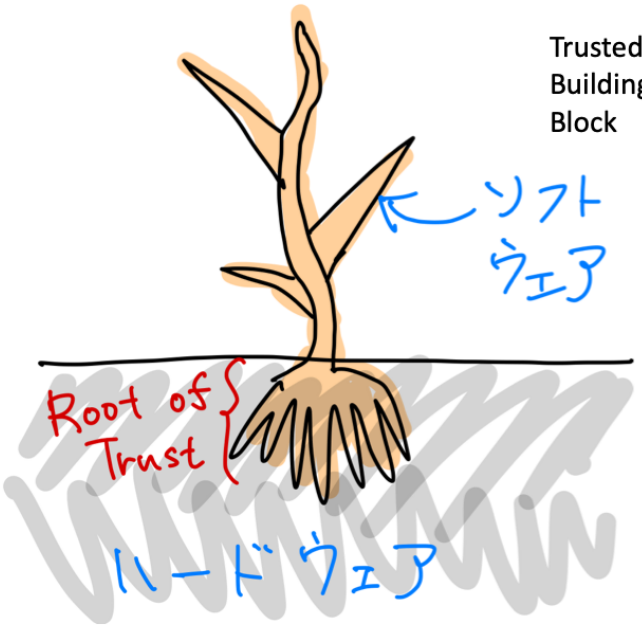
講演４
プラットフォームで実装されるトラスト

プラットフォームに組み込まれて行くデジタルトラストアーキテクチャ

垣内 由梨香 氏
（Microsoft Corporation セキュリティ レスポンスチーム セキュリティ プログラム マネージャー）

「デジタルトラストに対応するコンピュータアーキテクチャの変化」
コンピュータアーキテクチャ自体に暗号技術（主に公開鍵暗号技術）が取り込まれて行く
→　デジタル・トラストアーキテクチャ

Root Of Trust



宮澤のイメージ
本来は「信頼の根幹」という意味

Trusted Building Block

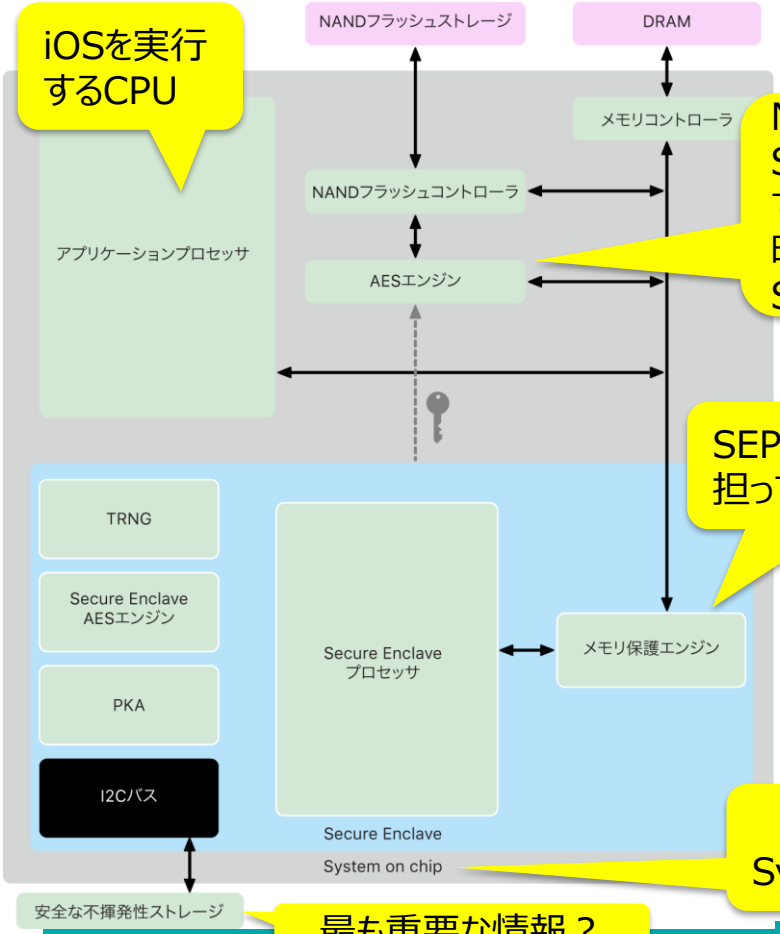
- Root Of Trust for Measurement
  - **完全性**を確認する計測プログラム
  - BIOSのROMやCPUのマイクロコード
- Root Of Trust for Report
  - **機器認証**できる形での**完全性報告**のための証明書
  - TPM
- Root Of Trust for Storage
  - 外部ストレージへ**暗号化保存**する暗号鍵
  - TPM

- ソフトウェアの完全性の木を成長させる
  - Chain Of Trust
- 計測のタイミング異なるRTM
  - Static RTM(BIOS + TPM)：電源起動直後
  - Dynamic RTM (Intel TXT)：任意タイミング

詳しくは後半で！

出典： PKI & TRUST Days online 2021 「デジタル社会におけるトラスト」
第１日目：2021年4月15日（木）テーマ：変貌するトラストアーキテクチャ
「トラストを確立する技術の概要 ～ どのような技術がなぜ作られてきたのか ～」
宮澤 慎一 氏（セコム株式会社 IS研究所 主務研究員）
https://www.insa.org/seminar/pki-day/2021/data/0415miyazawa.pdf

Apple のM1チップ(SoC)の中のSEP（セキュアエンクレーブプロセッサー）

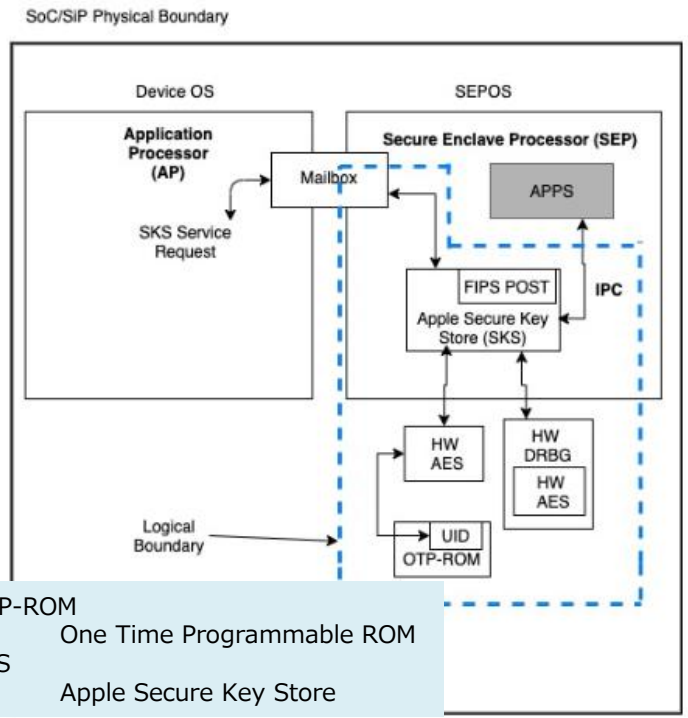


- 「セキュアエンクレーブプロセッサー」というネーミングはミスリードかも？？
  - エンクレーブ・TEE自体は、アプリケーションプロセッサーのメモリ空間上にある？？
  - エンクレーブを設定するのは、「セキュアエンクレーブプロセッサー」の役割？？

出典
Appleプラットフォームのセキュリティ　2021年5月
Secure Enclave
https://support.apple.com/ja-jp/guide/security/sec59b0b31ff

チップの中の境界線防御

境界線防御を否定するゼロトラストネットワークは、
こうした「チップ内の境界線防御」に依存することになる



OTP-ROM
One Time Programmable ROM
SKS
Apple Secure Key Store

Figure 1: Cryptographic Module Block Diagram

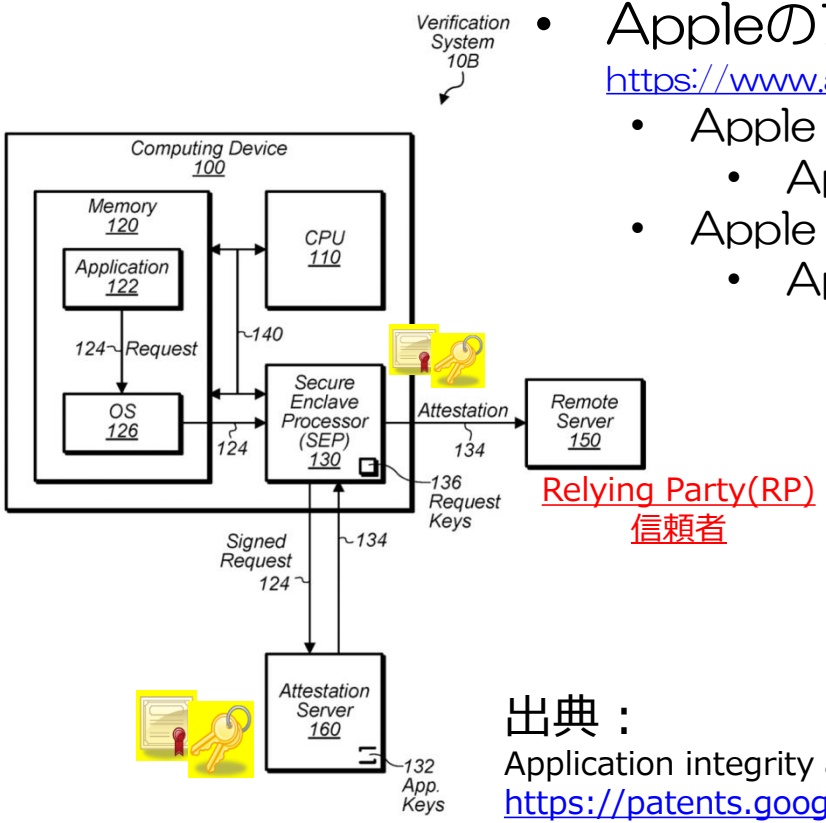
- physical boundary
  - メインCPU、セキュアエンクレーブプロセッサーなどを内包したSoC
  - UIDとcryptographic boundary内で生成される暗号鍵となどと不可分
- cryptographic boundary （Logical Boundary）
  - 暗号鍵などを内包し、暗号演算（主にデジタル署名）は、cryptographic boundaryのハードウェア境界線内で行う
    - 暗号鍵（署名鍵、暗号化鍵など）は、boundaryから外に出ない
  - 耐タンパー性などを有する

チップ外のboundary（Trusted boundary）
- cryptographic boundary内の署名鍵で署名されたデータ、暗号化鍵で暗号化されたデータ
- TEE, SGXのエンクレーブ（date in use の暗号化）等

出典：CMVP **Apple Secure Key Store Cryptographic Module v10.0 FIPS 140-2 Non-Proprietary Security Policy**
https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3858.pdf

出典： SEP：Secure Key Store のセキュリティ認証
https://support.apple.com/ja-jp/HT209632

セキュアエンクレーブを利用したリモートアテステーション



- Appleのプライベート**PKI**
  https://www.apple.com/certificateauthority/private/
  - Apple App Attestation Root CA
    - Application integrity attestation用のCA
  - Apple WebAuthn Root CA
    - Apple Webauthn（FIDO2)用のattestation用のCA

Relying Party(RP)
信頼者

Apple App Attestation??

出典：
Application integrity attestation
https://patents.google.com/patent/US20200159966A1/

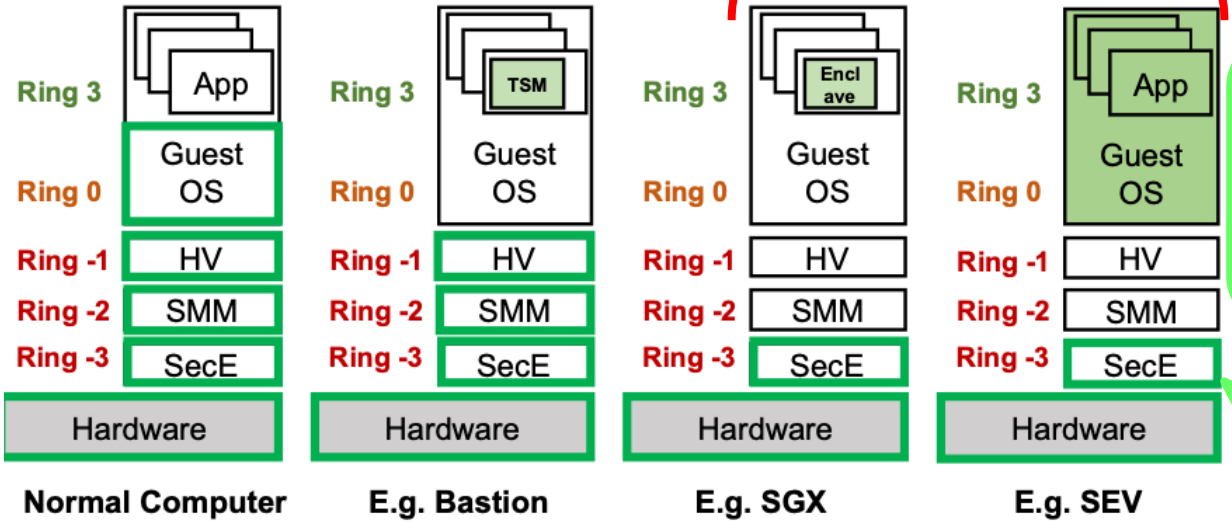
Ring-3 が作り出すリングプロテクションに依存しないセキュリティ
→このセキュリティモデルが作り出す新たなトラストモデル、ビジネスモデル

信頼される安心を、社会へ。SECOM

Breaking Linear Hierarchy of Protection Rings

Examples of architectures that do and don't have a linear relationship between privileges and protection ring level:

2021年現在、このふたつのハイブリッドなコンフィデンシャルコンピューティングが注目されている。



Ring -3 Platform management engine, retroactively named "ring -3", actually runs on a separate management processor.

Security Engine (SecE) can be something like Intel's ME or AMD's PSP.

出典:
Securing Processor Architectures :
https://caslab.csl.yale.edu/tutorials/asplos2021/asplos2021_tutorial_part2_public.pdf

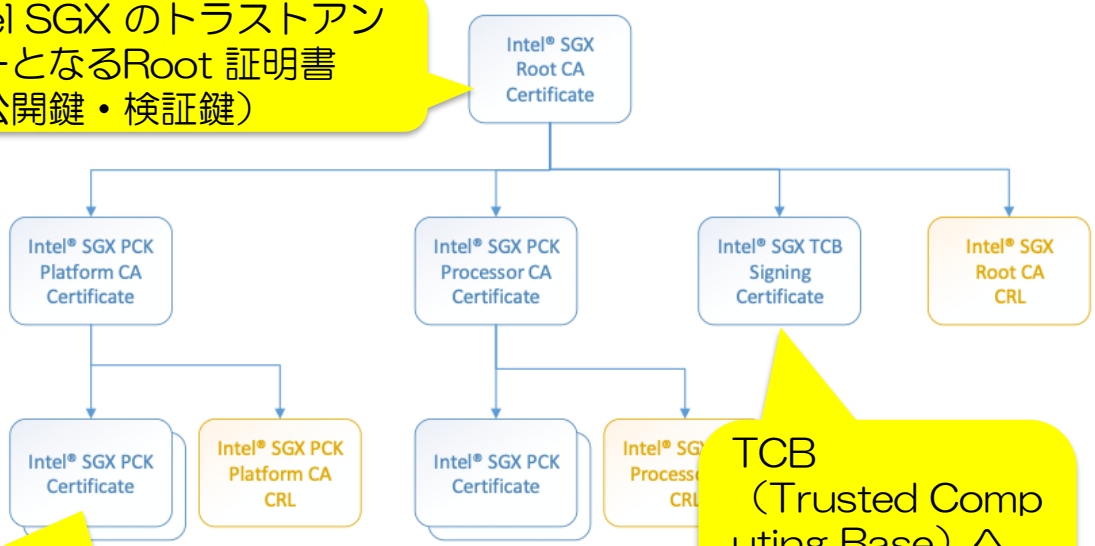
Securing Processor Architectures Tutorial – ASPLOS 2021
© Jakub Szefer 2021

13

Ring-3に組み込まれるPKI　　Intelの描くゼロトラスト？

CPUは、自分自身組み込まれた公開鍵（検証鍵）を頼りに自律的にエンクレーブを作り出す？？
ゼロトラスト環境に置かれるIntel SGX CPUは如何に外界をトラストするのか？

Intel SGX のトラストアンカーとなるRoot 証明書（公開鍵・検証鍵）

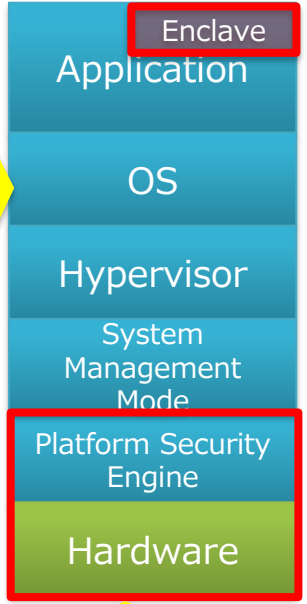


ure 2-1: Certificate Hierar

SGXのプラットフォーム（TCB等のアテステーション証明書）

TCB（Trusted Computing Base）へのコード署名に利用される公開鍵証明書？？

出荷されたCPUは、CPUを組み込むデバイスも製造者も、サービスもトラストせず、トラストアンカーとなる「公開鍵・検証鍵」から検証できるものだけをトラストしてエンクレーブまでを作る？？



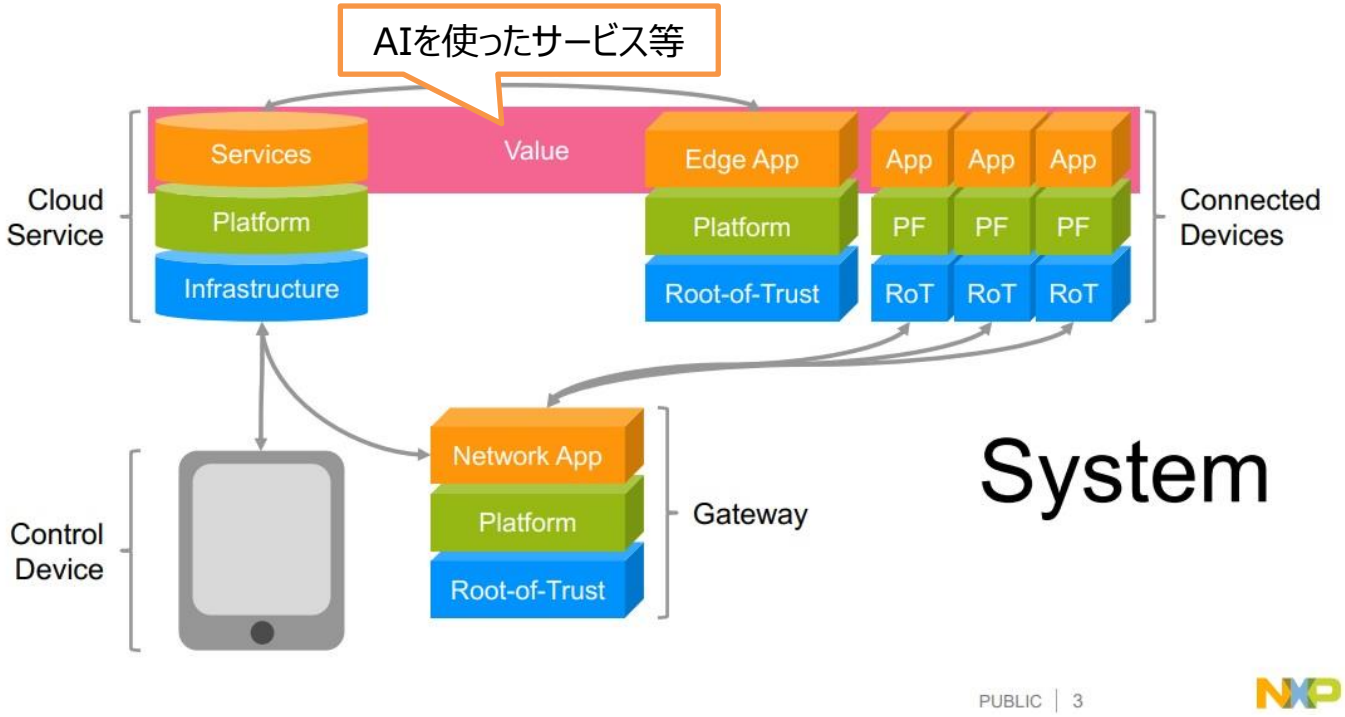
トラストアンカーとなるRoot証明書（公開鍵・検証鍵）が組み込まれたCPU

出典：　Intel® SGX PCK Certificate and Certificate Revocation List Profile Specification
https://download.01.org/intel-sgx/latest/dcap-latest/linux/docs/Intel_SGX_PCK_Certificate_CRL_Spec-1.4.pdf

IoTデバイス＆プラットフォームに組み込まれる トラストのメカニズム

- トラストのメカニズム・複雑性を縮減するメカニズムが、デバイスに組み込まれていく
  - Hardware Root Of Trust
  - Chain Of Trust　--　基本的には、HWRoTと起点に署名の連鎖と、その検証
  - セキュアブート・トラステッドブート
  - Trusted Execution Environments（TEE、信頼できる実行環境）
- リモートアテステーション　--　サイバーフィジカルシステムにおける
  - 遠隔からのデバイスの信頼性（trustworthiness）の検証
    - ＃知りたい信頼性（trustworthiness）は、様々

サイバーフィジカルシステムにおけるトラストのためのプラットフォームセキュリティの進化



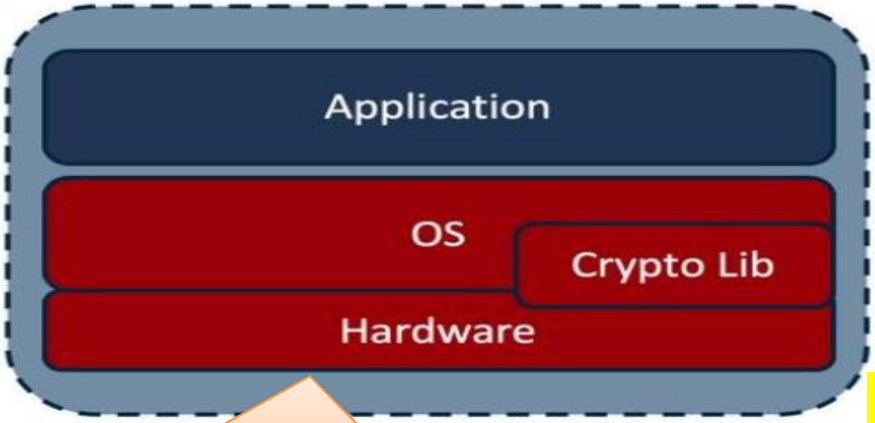
- IoTプラットフォームセキュリティ
  - ＃IoTプラットフォームの台頭にともなうIoTプラットフォームセキュリティの重要性
- HWRoT
  - HardWare Root of Trust

出典：
https://docbox.etsi.org/Workshop/2019/201906_ETSISECURITYWEEK/1806_CYBERSECURITY_POLICYACTIONS/02_CYBERSECURITYACT_INDUSTRIALIoT/VETILLARD_IIoT_Panel.pdf

サイバーフィジカルシステムにおけるトラストのための プラットフォームセキュリティの進化

境界線は、
・（従来からの）ハードウェアとソフトウェア間ではなく、
・IoTプラットフォームとIoTアプリケーション間に
存在する。

1.2 Terms used in this document



プラットフォームとしての
ハードウェアとソフトウェアは不可分

- IoTデバイスの認証（certification） → 制度的動向でもある。
  - ＃IoTデバイスのセキュリティに関する認証（certification)とトラストの関係
- IoTプラットフォームセキュリティの認証
  - Security Evaluation Standard for IoT Platforms (SESIP)

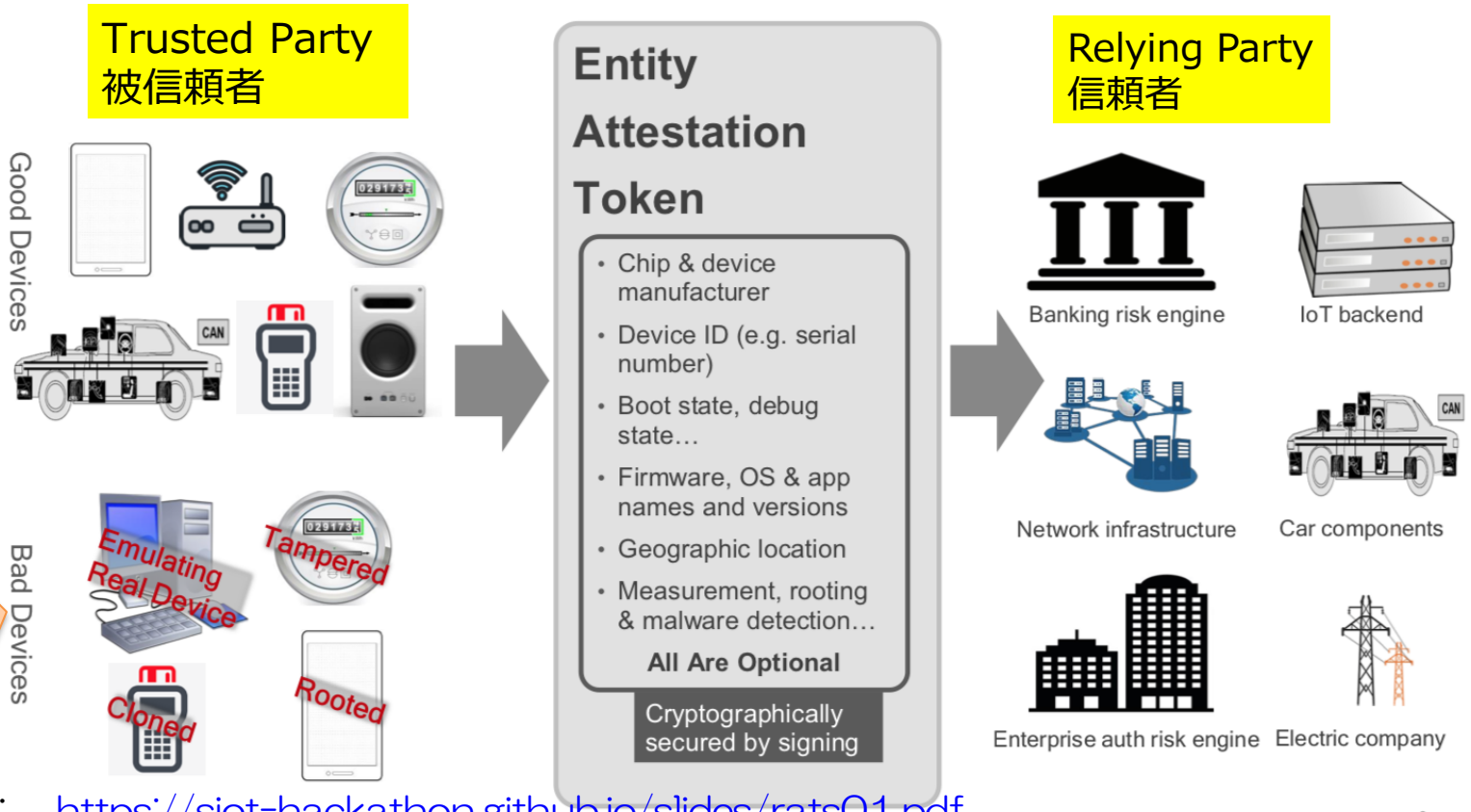
出典： TrustCB Scheme Procedures for SESIP Version 2.0
https://trustcb.com/download/trustcb-scheme-procedure-sesip-2-0/

サイバーフィジカルシステムにおけるトラストのためのプラットフォームセキュリティの進化

リモートアテステーション　（Remote Attestation）

Relying Party（信頼者）からみたトラストの観点からの
Bad devices

リモートアテステーションには、使えない。



出典：　https://siot-hackathon.github.io/slides/rats01.pdf

プラットフォームに実装されるトラスト：Appleの場合

エンクレーブ・TEEを中心に垂直統合を進める
Appleにおけるトラストの実装

購入したApple 製品は、購入者のモノ？？
ハードウェアも含めたインテグリティの実装

修理する権利の話
right-to-repair

- アップルの「純正」バッテリーへの交換であっても警告表示
  - 物理的攻撃（≒物理的な修理）に対する耐性がある。
  - サービスとしてのビジネスモデル（≒アップルの目指すビジネスモデル？？）では、ハードウェア攻撃とハードウェア修理が明確に区別できることが非常に重要

NEWS

iPhoneのバッテリー交換後の警告表示は、消費者の「修理する権利」を脅かす

iPhoneの最新モデルのバッテリーをユー
テリーに問題があることを示す警告が表
一側はセキュリティ上の問題や製品の破
張しているが、こうした動きが加速すれ
脅かす可能性がある。

出典：iPhoneのバッテリー交換後の警告表示は、消費者の「修理する権利」を脅かす
https://wired.jp/2019/08/22/apple-iphone-battery-service-alerts/

- ハードウェアセキュリティが必須となる
  - OTAが必須となる自動運転車
  - AppleWatchのようなAI技術等を駆使した（したい）医療デバイス
  - *#型式証明のパラダイムシフト*

Your Computer Isn't Yours

https://sneak.berlin/i18n/2020-11-12-your-computer-isnt-yours.ja/

- きたよ。ついに起こった。気がついたかい？
- もちろん、リチャード・ストールマンが 1997 年に予言した世界のことを言ってる。コリイ・ドクトロウが警告したものでもある。
- 最近のバージョンの macOS では、君はコンピューターの利用ログを記録されていて、ログデータを送信されることなしには、電源を入れてコンピューターを使うことも、テキストエディターや電子書籍リーダーを起動して書いたり読んだりすることもできない。
- 最近のバージョンの macOS では、君が実行しているすべてのプログラムのハッシュ値（固有識別子）を OS が Apple に送信していることがわかった。多くの人はこのことに気がついていなかった。なぜならログの送信はこっそり行われていて失敗したときも痕跡を残さないし、君がオフラインのときには何もしないようになっているからだ。しかし今日、ログ送信先のサーバーが不調をきたし、プログラムが障害回避処理のパスを通らなかったせいで、インターネットに接続した状態の Mac ではアプリを起動することができなかった。
- ログ送信処理はインターネット経由で行われているから、サーバーは君の IP アドレスを知ることができるし、もちろんそのログ送信処理がいつ行われたかも把握できる。 IP アドレスからは都市や ISP レベルの大体の位置情報がわかるし、こんな感じの情報でテーブルを組むことができる。
- 日付、時刻、コンピューター、 ISP 、市、州、アプリケーションハッシュ
- Apple は（もしくはそれ以外の誰だって）これらのハッシュ値は調べることができる。 App Store にあるアプリすべて、 Creative Cloud アプリ、 Tor ブラウザー、クラッキングもしくはリバースエンジニアリングツール、何でもだ。
- つまり Apple は君がいつ家にいるかわかるってことだ。君がいつ仕事に行ってるかも。どんなアプリをそこで起動して、どのくらいの頻度で使っているかも。君がいつ Premier を友だちの家の Wi-Fi ごしに開いたか、いつよその街のホテルで Tor ブラウザーを起動したかを知っている。
- 「誰が気にするもんか？」君はそう言うだろう。
- えーっとね、これは Apple のことだけじゃないんだよ。 Mac から送られる情報は Apple の手元だけにとどまるわけじゃないんだ。
- これらの OCSP リクエストは暗号化されることなく送信されている。ネットワークを監視できる人は誰だって見ることができる。君の ISP や回線を盗聴してる人もだ。
- これらの情報はサードパーティー（ Akamai ）の CDN を経由して収集されている。
- 2012 年の 10 月から Apple はアメリカ軍の諜報機関がやってる PRISM スパイプログラムの一員になっていて、連邦警察と軍が望めば令状なしでこれらのデータへ自由にアクセスすることが可能になっている。彼らは 2019 年の前半に 18,000 回以上、後半には 17,500 回以上も情報照会を実施している。
- このデータは君の生活や習慣を解き明かすための十分な材料になるだろうし、君につきまとう誰かが君の生活行動パターンを突き止めるのを可能にするだろう。ある種の人にとってはこれは物理的な危険をもたらすことだってある。
- （続く）

Apple PKI

Apple established the Apple PKI in support of the generation, issuance, distribution, revocation, administration, and management of public/private cryptographic keys that are contained in CA-signed X.509 Certificates.

Apple Root Certificates

- Apple Inc. Root Certificate
- Apple Computer, Inc. Root Certificate
- Apple Root CA – G2 Root Certificate
- Apple Root CA – G3 Root Certificate

Apple Intermediate Certificates

- Apple IST CA 2 – G1 Certificate
- Apple IST CA 8 – G1 Certificate
- Application Integration Certificate
- Application Integration 2 Certificate
- Application Integration – G3 Certificate
- Apple Application Integration CA 5 – G1 Certificate
- Developer Authentication Certificate
- Developer ID Certificate
- Software Update Certificate
- Timestamp Certificate
- WWDR Certificate (Expiring 02/07/2023 21:48:47 UTC)
- WWDR Certificate (Expiring 02/20/2030 12:00:00 UTC)
- Worldwide Developer Relations – G2 Certificate

Certificate Revocation Lists

- Apple Inc. Root CRL
- Apple Computer, Inc. Root CRL
- Software Update CRL
- Timestamp CRL
- Worldwide Developer Relations CRL

Certificate Policy (CP) and Certification Practice Statements (CPS)

Apple Root CA:

- Apple Certificate Policy
- Application Integration CPS
- Developer Authentication CPS
- Developer ID CPS
- Software Update CPS
- Timestamp CPS
- Worldwide Developer Relations CPS

Apple Public CA:

- Apple Public CA CPS

Audit Reports

Certification Authorities WebTrust

WebTrust for Certification Authorities:

- WTCA
- WTExternalRoots

Certification Authorities WebTrust BR - SSL

WebTrust for Certification Authorities – SSL Baseline with Network Security:

- WTBR

Apple Root Certificate Program

To better protect Apple customers from security issues related to the use of public key infrastructure certificates and enhance the experience for users, Apple products use a common store for root certificates. You may apply to have your root certificate included in Apple products via the Apple Root Certificate Program.

Contact

Contact the Apple PKI team at contact_pki@apple.com.

信頼される安心を、社会へ。

SECOM

Appleの製品・サービスのビジネスモデル＆トラストを支えるApple のPKI

- Apple Root CA
  - Apple Application Integration CA (AAI Sub-CA)
  - Worldwide Developer Relations CA (WWDR Sub-CA)
  - Software Update Sub-CA
  - Developer ID Sub CA
  - General Timestamp CA

出典：
https://www.apple.com/certificateauthority/

Apple Root CA

Developer ID Sub- CA

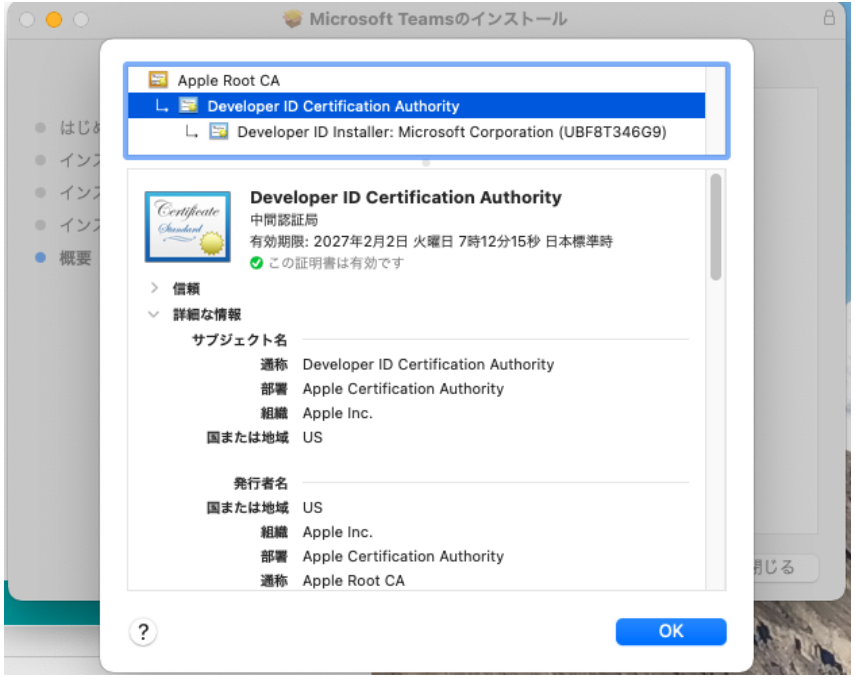
2.2. COMMUNITY AND APPLICABILITY

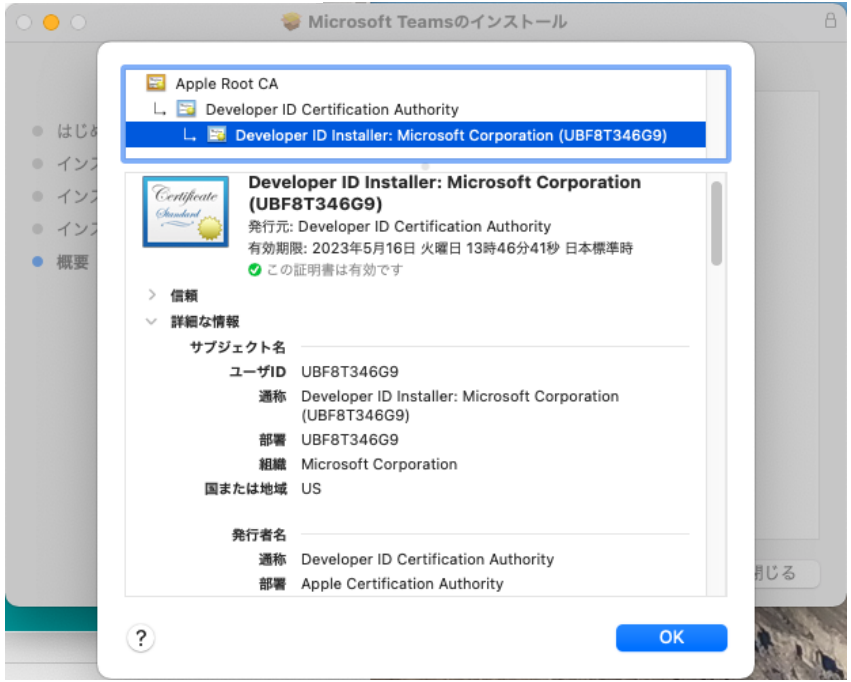
This CPS is applicable to the following certificates issued by the Developer ID Sub-CA:

- Developer ID Installer Package Signing Certificates
- Developer ID Application Code Signing Certificates
- Developer ID Application and Kernel Extension Code Signing Certificates

Certificates used exclusively for functions internal to Apple Products and/or Apple processes are not included within the scope of this CPS.

出典：
https://images.apple.com/certificateauthority/pdf/Apple_Developer_ID_CPS_v3.1.pdf





Appleの製品・サービスのビジネスモデル＆トラストを支える Apple のPKIから発行される様々なデジタル証明書

信頼される安心を、社会へ。
SECOM

- WWDR iOS Software Development Certificates (“iOS Development Certificates”)
- WWDR iOS Software Submission Certificates (“iOS Submission Certificates”)
- WWDR Apple Push Notification service Development SSL Certificates (“Development SSL Certificates”)
- WWDR Apple Push Notification service Production SSL Certificates (“Production SSL Certificates”)
- WWDR Push Certificate Signing Request Signing Certificates (“Push CSR Signing Certificates”)
- WWDR Safari Extension Signing Certificates (“Safari Certificates”)
- WWDR Mac App Development Certificates (“Mac App Development Certificates”)
- WWDR Mac App Submission Certificates (“Mac App Submission Certificates”)
- WWDR Mac Installer Package Submission Certificates (“Mac Installer Package Submission Certificates”)
- Mac App Store Application Signing Certificates (“Mac App Store Application Certificates”)
- Mac App Store Installer Package Signing Certificates (“Mac App Store Installer Package Certificates”)
- Mac App Store Receipt Signing Certificates
- Mac Provisioning Profile Signing Certificates
- Pass Certificates
- Website Push Notification Certificates
- OS X Server Authentication Certificates
- VoIP Services Push Certificates
- Apple Pay Merchant Certificates
- Apple Pay Pass Certificates
- TestFlight Distribution Certificates
- WatchKit Services Certificates
- Apple Pay Provisioning Encryption Certificates
- Enhanced Pass Certificates
- tvOS Application Signing Certificates
- WWDR Apple Push Services Client Authentication G2 Certificates
- Apple Pay Merchant Client Authentication Certificates
- WWDR Apple Development Signing Certificates ("Apple Development Certificates")

出典：
https://images.apple.com/certificateauthority/pdf/Apple_WWDR_CPS_v1.22.pdf

Appleプラットフォームのセキ ュリティ（2021年5月）
Appleプラットフォームのセキュリティの概要
https://support.apple.com/ja-jp/guide/security/seccd5016d31

信頼される安心を、社会へ。
SECOM

- ハードウェアセキュリティと生体認証:　Secure Enclave、専用のAES暗号化エンジン、Touch ID、Face IDなど、Appleデバイスのセキュリティの基盤をなすシリコンやハードウェア
- システムのセキュリティ:　安全な起動、アップデート、およびAppleのオペレーティングシステムの継続的な動作を可能にする、統合されたハードウェア機能とソフトウェア機能
- 暗号化とデータ保護:　デバイスを紛失したり盗まれたりした場合や、不正なユーザまたはプロセスが使用したり変更したりしようとした場合でもユーザデータを保護するアーキテクチャと設計
- Appのセキュリティ:　Appの安全なエコシステムを実現し、プラットフォームの整合性を損ねることなく安全にAppを実行できるようにするソフトウェアおよびサービス
- サービスのセキュリティ:　ID、パスワード管理、支払い、通信、紛失したデバイスの発見のためのAppleのサービス
- ネットワークのセキュリティ:　安全な認証と転送データの暗号化を可能にする業界標準のネットワークプロトコル
- デベロッパキットのセキュリティ:　プライバシーを守って家や健康を安全に管理するため、およびAppleのデバイスとサービスの機能を他社製Appにまで拡張するためのフレームワークの「キット」
- 安全なデバイス管理:　Appleデバイスを管理し、不正使用を防ぎ、紛失または盗難時にリモートワイプを可能にする方法

unauthorised person or process
platform integrity
secure authentication

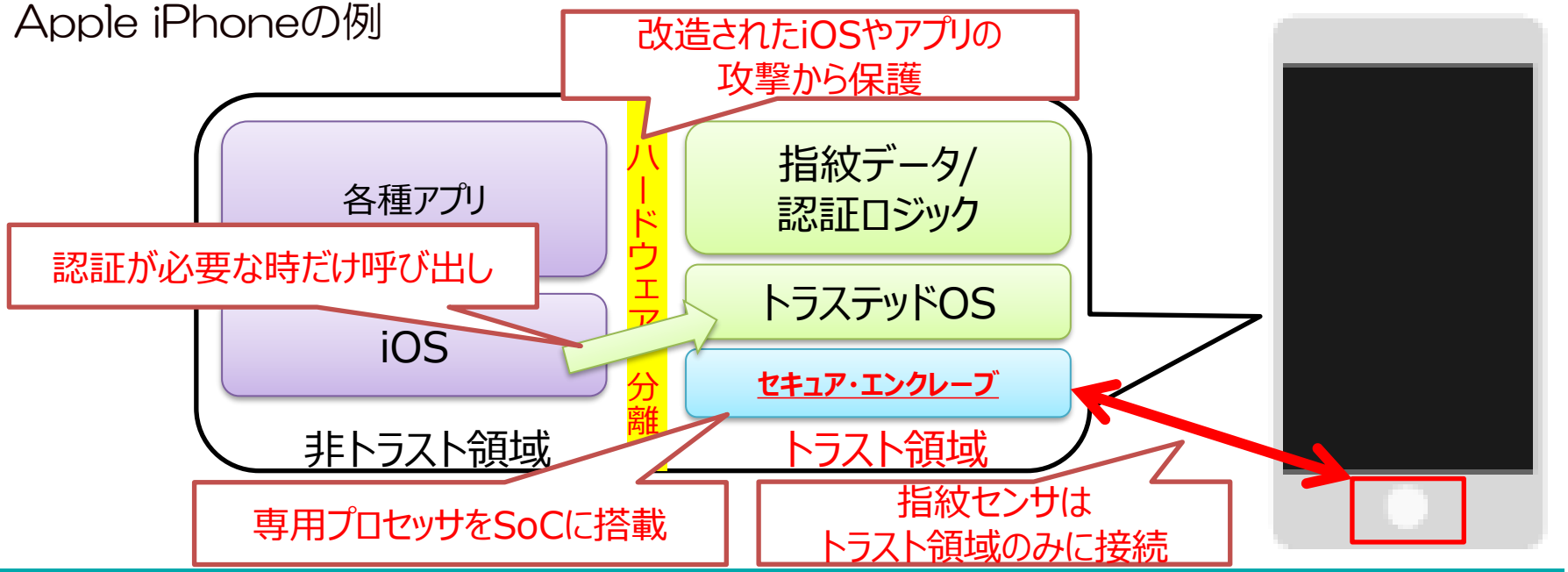
Hardware Security and Biometricsの意味するところ

信頼される安心を、社会へ。
SECOM

- ハードウェアにより通常アプリと隔離されたトラスト領域
- トラスト領域：通常アプリやOSが改ざん等の侵害されても影響を受けない

決済や認証、暗号化処理等の重要な処理・データを配置し、通常アプリと連携

- Apple iPhoneの例



MacおよびiPadのハードウェアマイク切断

https://support.apple.com/ja-jp/guide/security/secbbd20b00b/1/web/1#spaceexplored

- Apple T2セキュリティチップを搭載したすべてのMacポータブルは、蓋が閉じられるたびにマイクを確実に無効にするハードウェア切断機能を備えています。T2チップを搭載した13インチのMacBook ProおよびMacBook Airコンピュータと15インチのMacBook Proポータブル（2019年以降）では、この切断機能はハードウェアのみに実装されています。macOSでルート権限またはカーネル権限を持つソフトウェアとT2チップ上のソフトウェアも含め、どのソフトウェアも蓋が閉じられているときにはマイクを使用できません。（カメラは、蓋が閉じられているときには視野が完全に覆い隠されるため、ハードウェアで切断されません。）
- 2020年以降のiPadのモデルもハードウェアマイク切断に対応しています。MFI準拠のケース（Appleで販売しているものなど）がiPadに装着され、閉じているときには、マイクがハードウェアで切断されるため、マイクのオーディオデータはどのソフトウェアからも使用できなくなります。iPadOSのルートまたはカーネル権限を使用しても、ファームウェアが危殆化された場合も使用できません。

心電図機能を持ったApple （watch) の場合
Apple Secure Key Store Cryptographic Module, v1.0 FIPS 140-2 Non-Proprietary Security Policy

Apple Watch Series 1 with Apple S1P CPU	SEPOS for S1P under watchOS 4
Apple Watch Series 3 with Apple S3 CPU	SEPOS for S3 under watchOS 4

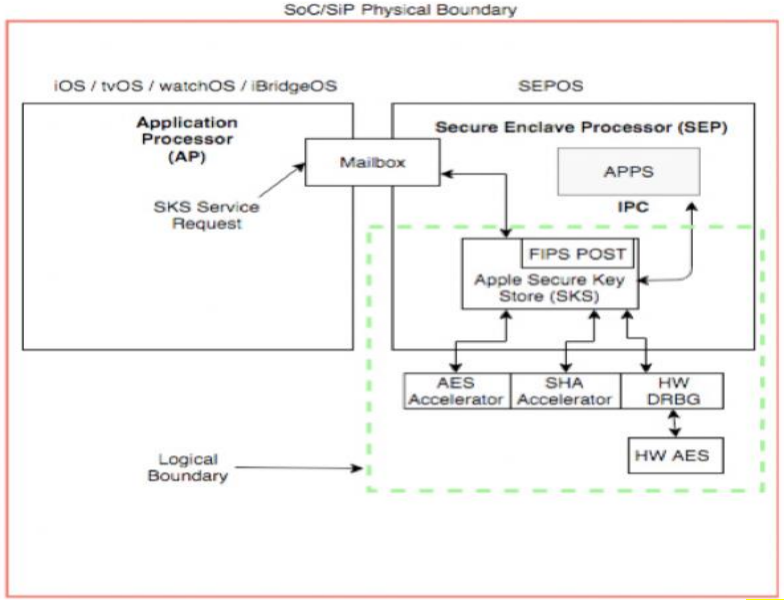


Figure 1: Cryptographic Module Block Diagram

https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3223.pdf

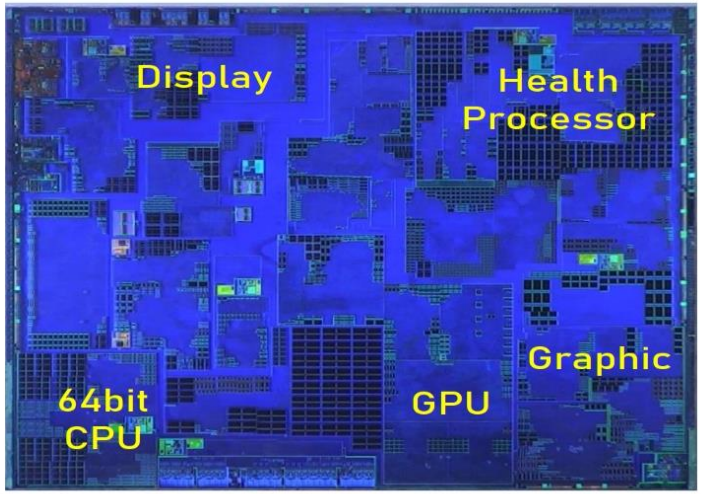
配線層剥離

300φ 1508個
Silicon Cost ¥576

TSMC 10nm Process

CPU
64bit Dual Core
2 x Faster then S3

GPU
Display Controller
Audio Controller
DDR Controller



出典： テカナリエレポート TLSR242号 2018年10月26日

SoCに組み込まれたセキュアエンクレーブ・プロセッサーは、Apple watch を利用する様々なサービス（医療サービスなどの規制産業も含む）にトラストの起点を提供している。