超スマート社会実現のための トラスト・テクノロジー

2018年11月5日

松本 泰
JT2A副代表/
JNSA PKI相互運用技術WGリーダー/
セコムIS研究所

- (1) PKI day における議論の振り返り
  - 第１回　PKI day 2005　からの「技術中心の議論」
  - 2010年頃からの「法制度も含めた議論」
  - ここ2,3年の「社会の変化（超スマート社会への変化）に伴う議論」
- (2) 超スマート社会実現のためのトラストテクノロジー
  - #来年４月に開催予定の「PKI day 2019」の予告？？
  - 「サイバー空間とフィジカル空間が高度に融合した社会」におけるサービスイノベーションと、そのためのトラストテクノロジー

PKI day における議論の振り返り

- 第１回　PKI day　2005　からの「技術中心の議論」
  - 相互運用技術・インターオペラビリティ
- 2010年頃からの「法制度も含めた議論」
  - 業界、分野を横断するための上位のポリシーの整合、LoA等
- ここ2,3年の「社会の変化（超スマート社会への変化）に伴う議論」
  - 社会自体の変化、パラダイムシフト

PKI day における議論の振り返り

年	PKI day テーマ
2005	PKI技術最新事情
2006	PKIの展開と最新技術動向
2007	PKIの過去・現在・未来
2008	PKIの標準から実装まで 最新動向
2009	さまざま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 ・PKIへの攻撃とその対応
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」
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

技術中心の議論

法制度も含めた議論

社会の変化に伴う議論??

社会基盤としてＰＫＩ

PKI Day 2010
社会基盤としてのPKI／PKIの10年

デジタル時代の
日本の社会？

効率的で、透明性があり
競争力のある社会？

目的

デジタル時代の
社会サービス

トラスト が必要な様々な社会サービス

デジタル時代の
社会基盤

社会基盤としてのトラストサービス　etc…

デジタル時代の
（信頼のための）
フレームワーク

標準化

実装

法制度

デジタル時代の
要素技術

暗号技術　etc..

２０１１年現在の状況？

PKI Day 2011-＜番号制度時代のPKI＞

JT2A

？？？

"Rough consensus and running code"

民事訴訟法は228条4項 「私文書は、本人又はその代理人の署名又は押印があるときは、真正に成立。。」

法制度等から
ニュートラルな
技術標準

技術標準

ギャップ

噛み合わない会話
共有されないビジョン

・既存のレガシーな法制度
・様々な管轄官庁の様々な業法

デファクト標準
としての実装

対極の実装

紙前提の制度
（の電子化）

強い影響

「電子署名法」、「e文書法」、「電子公証人制度」、「商業登記に基づく電子認証制度」、「住民基本台帳制度」、etc….

現実の実務からの乖離という問題

既存の慣習、権益が強すぎる問題

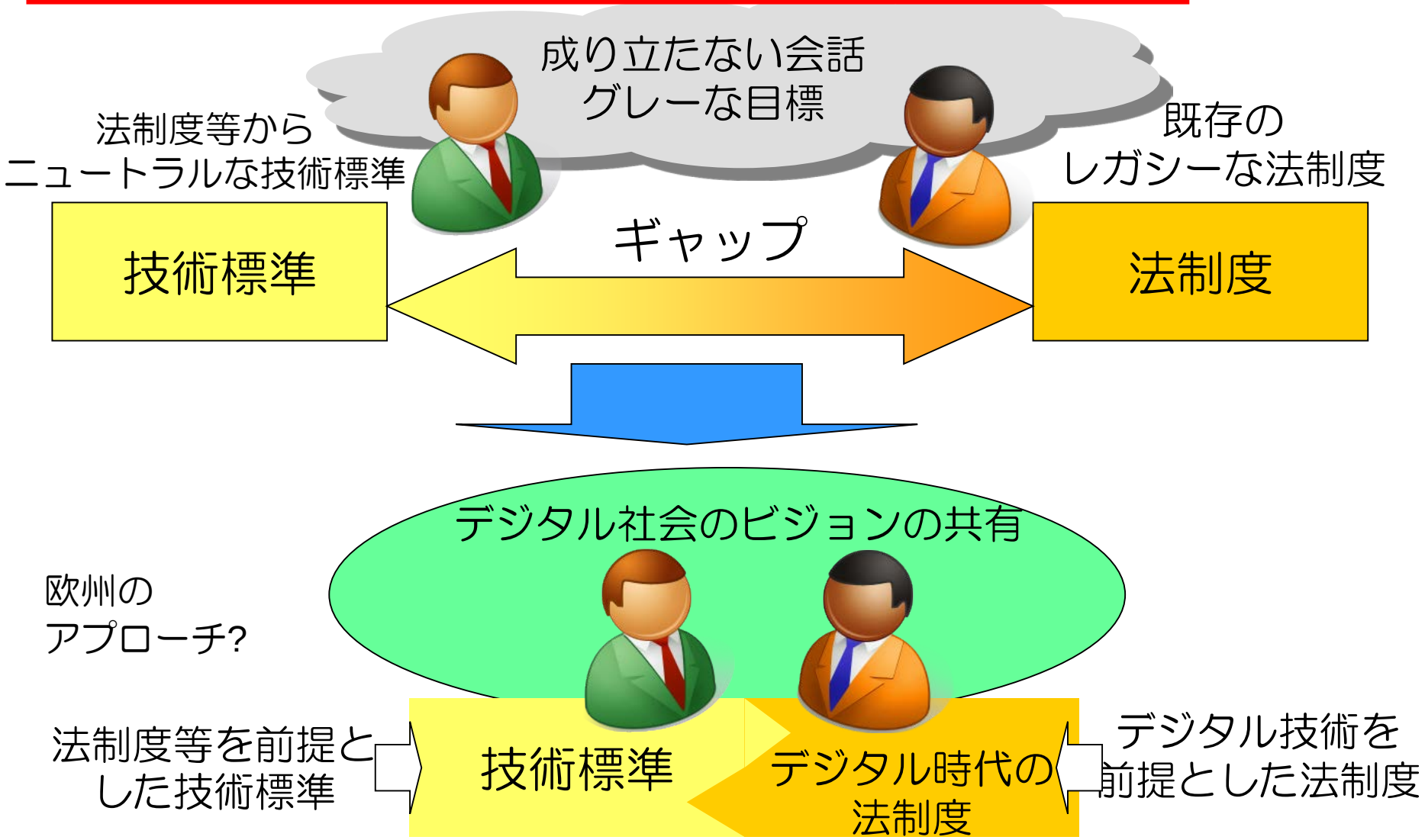
「光の道」で医療問題も教育問題も解決する？

番外編

現在の医療の問題点は、デジタル化以前の問題

技術と制度をかみ合わせるためには

PKI day 2012・我が国における信頼基盤の連携に向けて



PKI day 2015のオーバビュー

PKI day 2015サイバーセキュリティの要となるPKIを見直す

JT2A

3部　広がるサイバー空間に対応するPKIの新しい応用領域

時代の要請

マイナンバー制度の時代

ビッグデータ時代

IoT時代

サービスレイヤー

行政サービス
医療サービス
金融サービス
Webサービス

電子契約書
医療記録
電子領収書
プログラム（コード署名）

オープン化する制御システム
医療機器
ITS
車の車載器
IPルーティング

信頼が必要な情報連携サービス

信頼が必要なデジタルコンテンツ

数百億個のデバイスの多様な信頼関係

トラストレイヤー

eIDAS
電子署名
タイムスタンプ
電子シール
電子配布
Webサイト認証

Web trust for CA
Webサイト認証
DNSSEC
RPKI

（広義の）トラストサービス

トラストを構成する要素

デジタル社会のための法制度

法制度と整合性のある標準化

信頼のおける運用

セキュアな実装技術

暗号技術等のコア技術

1部 新しい時代の電子署名

2部 SSL/TLS実装の今とこれから

欧州・米国・日本

PKI day 2016マイナンバー時代のPKI

欧州
規制モデル

米国
市場モデル

トラストが必要なサービス

一般データ
保護規則

個人情報の連携・個人情報の利活用と保護

eIDAS規則

トラストサービス・レイヤー

ハイパー
ジャアアント
による支配？

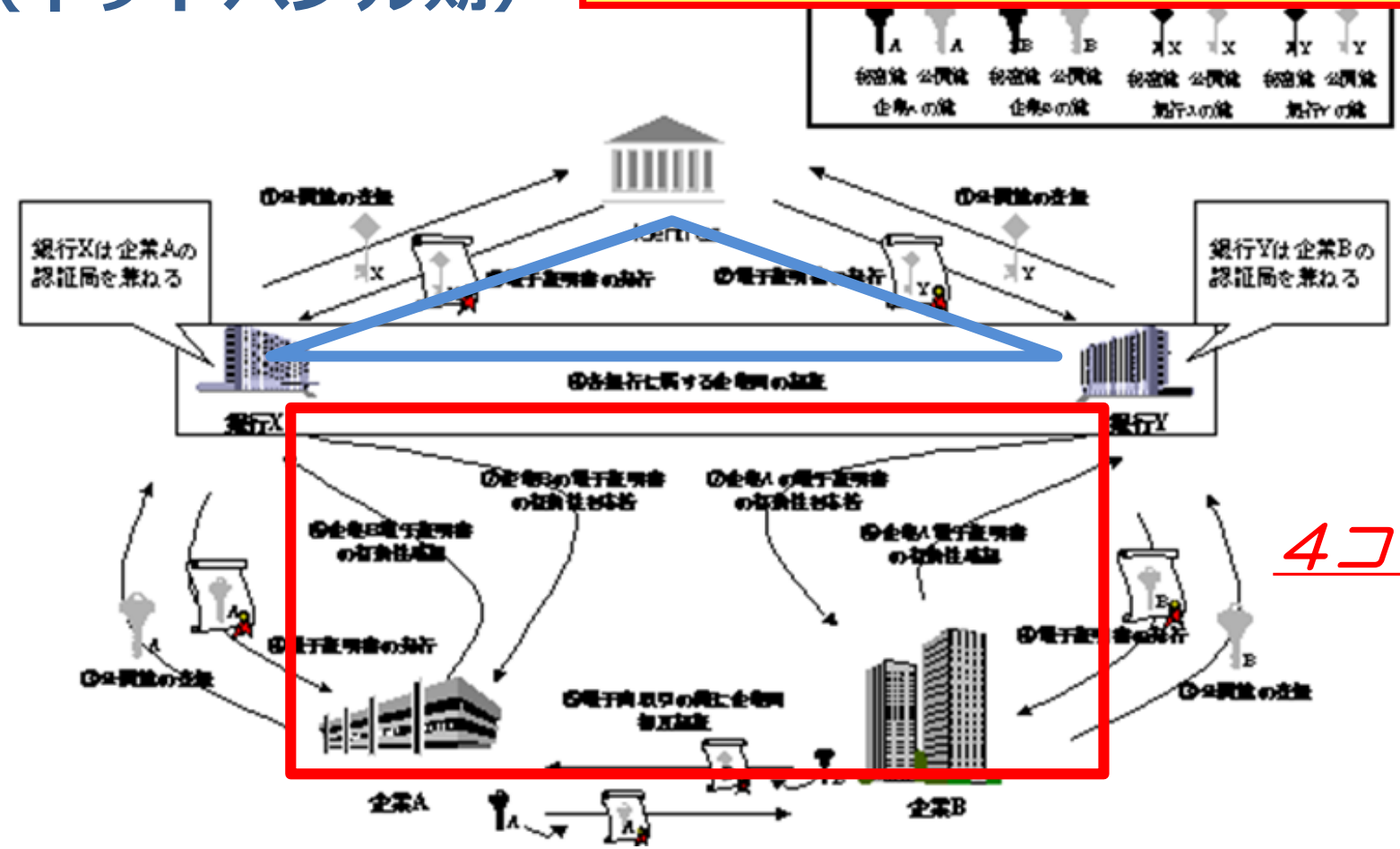
アイデンティティ管理（自然人、法人）
日本におけるマイナンバー制度等

大陸法的
アプローチ

英米法的
アプローチ

日本の立ち位置は？？

2000年頃のFintech??　Identrus（ネットバブル期）



HAT

4コーナー

４コーナーモデル　--　トランザクションに信頼を与える仕組み

HAT　--　信頼のおける（ポリシが整合した）金融機関を追加する仕組み

→デジタルデータのみで自動的にトランザクションを検証する

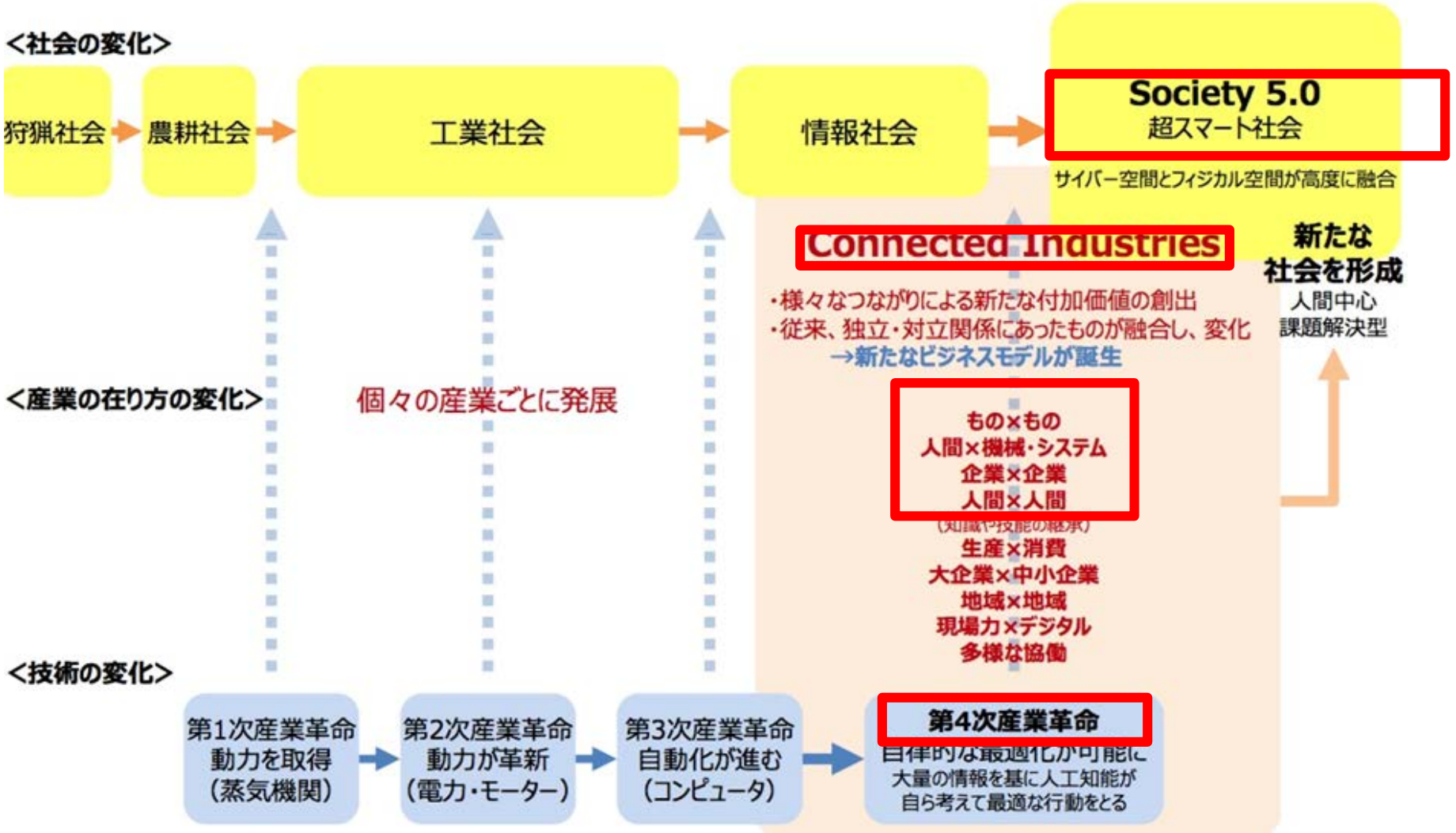
出典：　Identrusのイメージ https://www.ipa.go.jp/security/enc/digitalsignature/32_ED.htm

2017年度版「4コーナモデル+ HAT」の妄想？

- 2000年頃のIdentrusの 「4コーナモデル+ HAT」
  - 4コーナモデルの顧客の取引（異なるパーティ間の取引の仕組み）
    - ✓ 当時、４コーナモデルは成功せず、3コーナモデルで利用
    - ✓ ＃ブロックチェーンによる金融機関間の海外送金等と類似
  - HAT:　Identrusの**ポリシーに整合**した金融機関へCA証明書を発行
- では、2017年現在における「 4コーナモデル+ HAT 」を実装を妄想
  - 各金融機関のクレデンシャル管理
    - ✓ 犯罪収益移転防止法、KYC（Know Your Customer）対応
    - ✓ **リモート認証**は、**JPK利用者認証用証明書**、または、**FIDOトークン**？？
    - ✓ **本人と結びつきを保証したリモート署名のための仮名証明書**の発行
      - 仮名証明書は、何枚でも発行
      - 仮名証明書に対応したオンライン・ウォレットの秘密鍵管理
  - HATの実装
    - ✓ ポリシーを満足していることを示すCA証明書を金融機関のへ発行
  - 4コーナモデルの実装
    - ✓ 顧客は、仮名証明書を使い分けることができる。
    - ✓ **リモート署名サーバ**で署名したトランザクション(送金データ等）をブロックチェーン？？に書き出し

社会の変化に伴うトラストの概念の変化（１）

PKI day 2018　**超スマート社会**（Society 5.0）における**トラスト**の在り方



出典：http://www.meti.go.jp/committee/sankoushin/shojo/pdf/004_02_00.pdf

社会の変化に伴うトラストの概念の変化（２）

PKI day 2018　超スマート社会（Society 5.0）におけるトラストの在り方

- 情報化社会以前のトラスト
  - 人のコミュニティにおける信頼関係　⇒　face2face
  - 地域を超えた信頼関係、国と国の信頼関係　⇒　羊皮紙、紙、印鑑
  - 法制度：紙台帳と（信頼のおける）人の目視による判断、確定日付
- 情報化社会におけるトラスト　-- 制度設計が、紙台帳の延長上のまま？？
  - 紙台帳から電子データ/データベース
  - 人が入力（自然人、法人）するデータ　⇒　紙台帳と人の判断の延長上
  - 電子署名法　⇒　民事訴訟法228条４項におけるデジタル文書への適用
  - 証明：　自然人、法人、時刻、Webサイト、etc
  - トラストな環境　≒「物理的環境で守られた場所」,「物理的環境によるトラスト」
- 超スマート社会におけるトラスト　-- デジタルデータ前提の制度設計の社会へ？
  - 「紙台帳と人の目視による判断」の延長上ではない制度設計の必要性
  - IoTが吐き出すデータ、AI等による判断(そのエビデンス)
  - スマートコントラクト的なルールに従った処理（そのルールの信頼等）
  - トラストな環境　≒「物理的環境で守られた場所」からの脱却

社会の変化に伴うトラストの概念の変化（３）
サイバー空間とフィジカル空間が高度に融合した社会

JT2A

PKI day 2018　**超スマート社会**（Society 5.0）における**トラスト**の在り方

- 「暗号技術によるトラスト」とサービスイノベーション
  - ➢ 暗号技術は、セキュリティ対策というよりは、 サービスイノベーションにとって必要　　ex. ブロックチェーン？？
- 「物理的環境によるトラスト」
  - 典型的な「物理的環境によるトラスト」
    - 外部と遮断されフィジカルセキュリティにより守られた「トラステッドネットワーク」
  - 「物理的環境によるトラスト」の問題
    - ✓ 物理的環境、セキュリティのコスト、物理的制約
    - （物理的に）多数のステークホルダー間のトラストの実現が難しい
- 「暗号技術によるトラスト」 のビジネス上のメリット
  - 物理的制約がなくなる（少なくなる）
    - ✓ IoT+ 「暗号技術によるトラスト」は、フィジカル空間におけるサービスイノベーションを生む。
    - 自動車の場合： OTA(over-the-air)によるプログラムの更新

超スマート社会実現のための
トラスト・テクノロジー

（#来年４月に開催予定の「PKI day 2019」の予告？？）

- 「サイバー空間とフィジカル空間が高度に融合した社会」におけるサービスイノベーションと、そのためのトラスト・テクノロジー

超スマート社会における繋げることによる価値の創造
サイバー空間とフィジカル空間が高度に融合

フィジカル空間とサイバー空間を高度に融合させる
IoTサービスシステム ≒　CPS（Cyber Physical Systems）

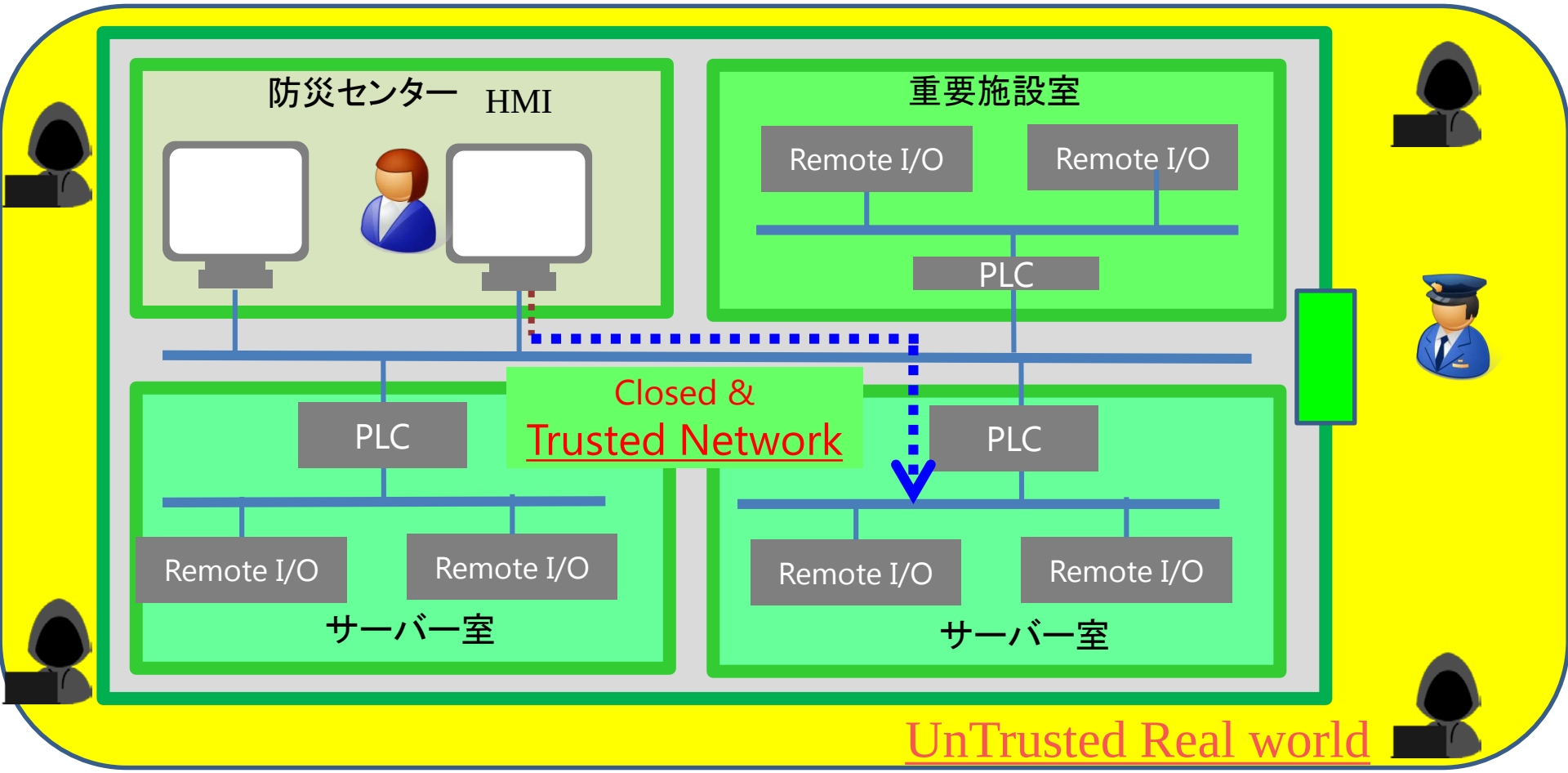
サイバーフィジカル・システムにおける セキュリティとトラストの関係

- セキュリティ対策
  - 主に、悪意ある第3者からの攻撃対策の観点

- トラスト
  - ステークホルダー・エンティティの信頼関係の構築の観点
    - トラスト・テクノロジーにより実装される信頼関係
  - サイバーフィジカル・システムにおいては、
    - 繋げることによる価値の創造のためには、IoTデバイスが、
      - 如何にして、繋がる相手を信頼するのか？
      - 如何にして、繋がる相手に信頼を伝えるのか？
    - これは実現したいビジネス・サービスモデルそのものであり、トラスト（信頼関係）こそが、価値を提供する
  - トラストテクノロジーは、価値を提供するサービスイノベーションのための技術

重要インフラにおけるトラスト（Trusted Network）セキュリティ区画とセキュリティ境界におけるアクセス制御

Closed & Trusted Networkのセキュリティ　≒　物理セキュリティ



こうした「Closed & Trusted Network」も、
価値の創造のために様々な接（Connected）
が求められつつある

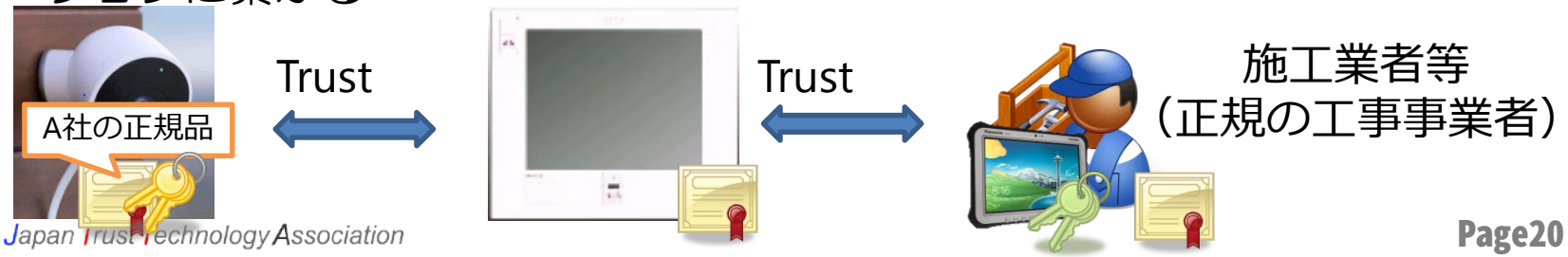
トラストな空間　セキュリティ区画

サイバーフィジカルシステムにおける暗号技術（トラストテクノロジー）によるトラスト

Trusted IoT device＆トラスト・テクノロジーで構成されたフィジカル空間上のセキュリティ区画

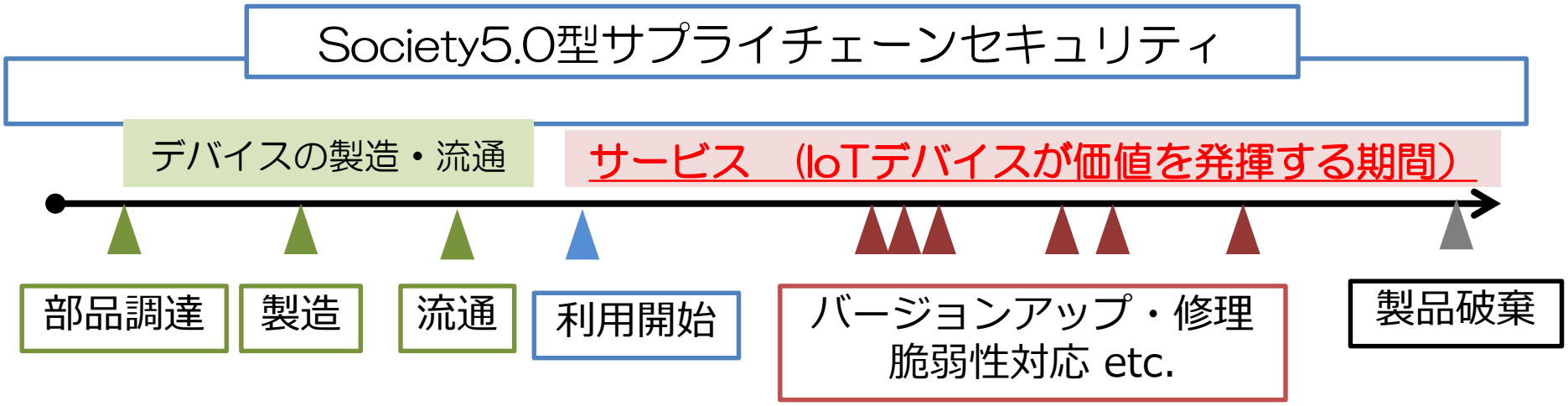
Trusted IoT deviceのためのトラスト・テクノロジー
（半導体の）ハードウェアセキュリティ＋信頼の起点（Root of Trust）

- ハードウェアセキュリティ
  - 信頼の起点となる暗号鍵等を、ハードウェアセキュリティで守る
  - 従来のICカード（スマートフォン）等の技術のIoTデバイスへの応用
  - （構成部品の多くが半導体(SoC)なので）大量生産による低コスト化が可能
    - ✓ 最終的には、シリコン原価
- 信頼の起点（Root of Trust）　⇒　Hardware Root of Trust (HWRoT)
  - IoTデバイスに格納された暗号鍵を信頼の起点（Root of Trust）として、様々な信頼関係（デバイス内、デバイス外のトラスト）を構築する。
    - ✓ IoTデバイス自身が、 Root of Trustを頼りに自律的に動作することにより、IoTデバイスの管理コストを最小限にする。
- 広域＋大量のIoTデバイスをセキュアで効率的な管理するためのHWRoTと、鍵管理・クレデンシャル管理システム　≒　（狭義の）トラストサービス
  - 従来の多くの「機器管理」 は、「物理的ゾーニング」「頑丈な筐体」「人手による管理」等が前提　⇒　ここのコストの低減が可能になり、サービスイノベーションに繋がる



時間軸：
IoTデバイスが生み出す価値・コスト・セキュリティ

製造からサービスにわたる長期のデバイス管理・暗号鍵管理が重要



個別のIoTデバイスの観点
長期の暗号鍵管理に耐えうる
ハードウェアセキュリティと
Root of Trust（信頼の起点）

→ Secure Boot
Secure Update

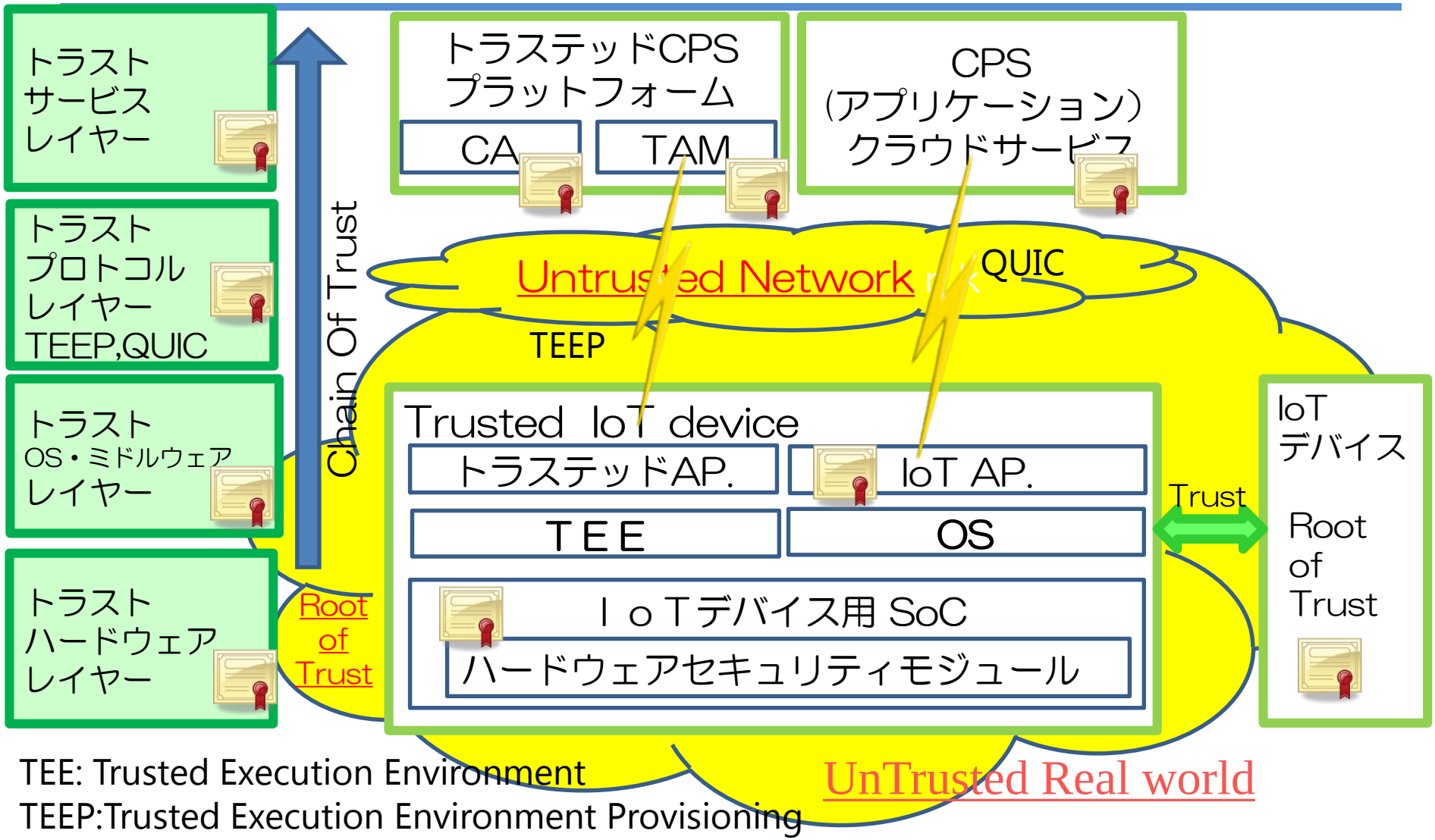
Trusted IoT device

サービスシステムからの観点
長期の信頼(=長期の暗号鍵管理)のおける運用

- アクセス制御・権限管理
- クレデンシャル管理
- 暗号鍵管理

トラストサービスの役割

トラストなサイバーフィジカルシステムのレイヤー構造



TEE: Trusted Execution Environment
TEEP:Trusted Execution Environment Provisioning
TAM : Trusted Application Manager
QUIC:

トラストサービス・レイヤーへの要求（ポリシーの整合）
多くのステークホルダーの信頼関係が必要となる
欧州のITS-Cにおける証明書発行と証明書ポリシー

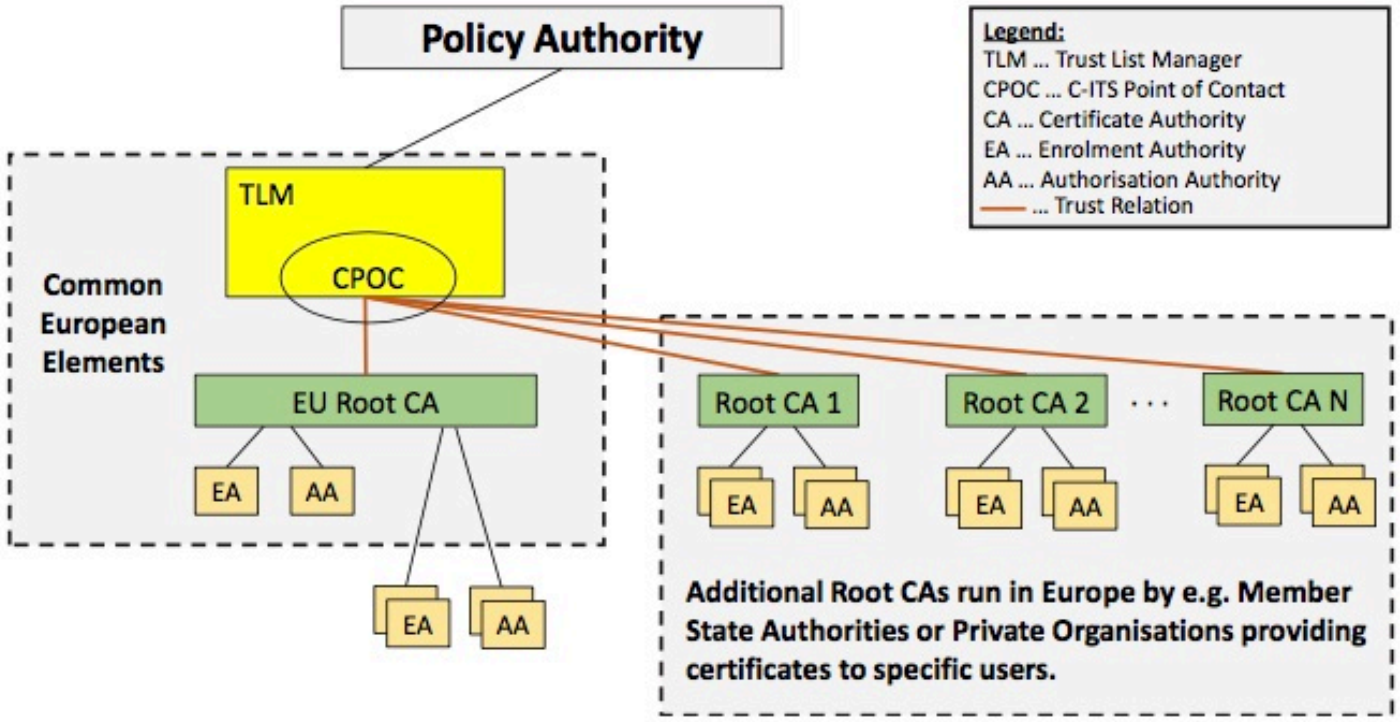


Figure 1: C-ITS Trust model architecture

出典： Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS) https://ec.europa.eu/transport/sites/transport/files/c-its_certificate_policy_release_1.pdf

多くのステークホルダーによる複雑な信頼関係が必要な「超スマート社会」にこそ、トップダウンなポリシーメイクによるトラストサービスが非常に重要になる。

超スマート社会実現のための トラスト・テクノロジー

- 我が国の施策として、第４次産業革命の対応、また、IoT/BD/AI等を駆使した超スマート社会（Society 5.0）といった構想が検討されています。
- この超スマート社会は、多様な人・モノ・サービスなどが繋がることにより新しい価値が創造と、社会の効率化、透明性等が目指された社会と言えます。
- 超スマート社会において、サイバーセキュリティーがより重要な役割を果たすことは間違いありませんが、その中でも「繋がることによる新しい価値の創造」の価値に大きく関わる技術がトラスト・テクノロジーになります。
- 例えば、数百億個のIoTデバイスが、単に繋がるだけで価値を生む訳ではなく、何らかの信頼関係が必要になります。
- 超スマート社会実現のためには、数百億個のIoTデバイスが価値を持つためのトラスト・テクノロジー、トラストサービスが望まれます。