PKI Day 2019

セコムIS研究所
Intelligent Systems Laboratory

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

2019 年　4月　17日

松本　泰　　セコム（株）ＩＳ研究所

PKI day 2019 までの歩み

セコム IS研究所
Intelligent Systems Laboratory

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	

PKI [illegible] ビュー

午後の部
トラストサービスの在り方

午前のの部
IoTのトラスト

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
[illegible]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

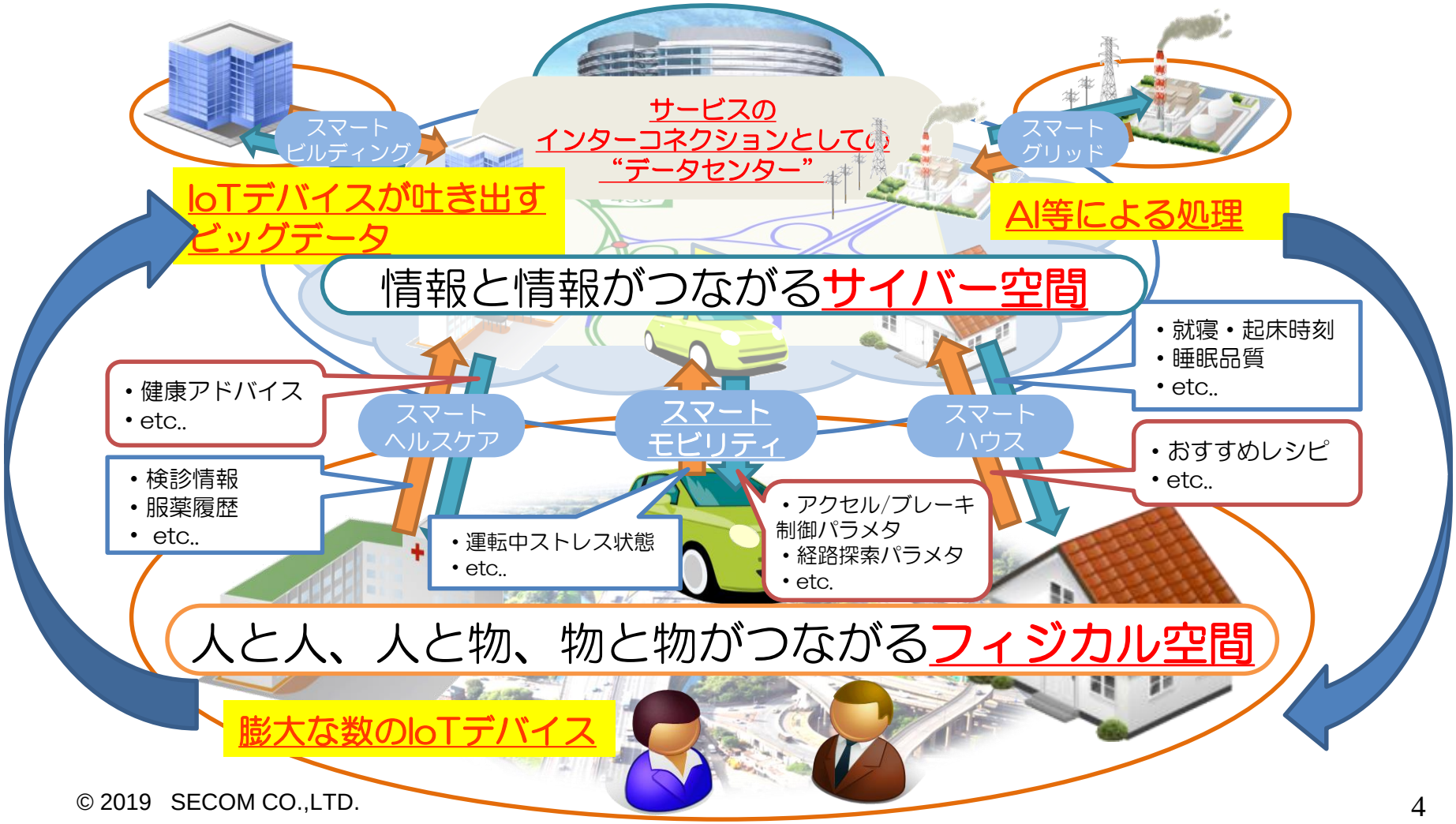
デジタル社会のための法制度
法制度と整合性のある標準化
信頼のおける運用
セキュアな実装技術
暗号技術等のコア技術

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

午前中の部　IoTのトラスト

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

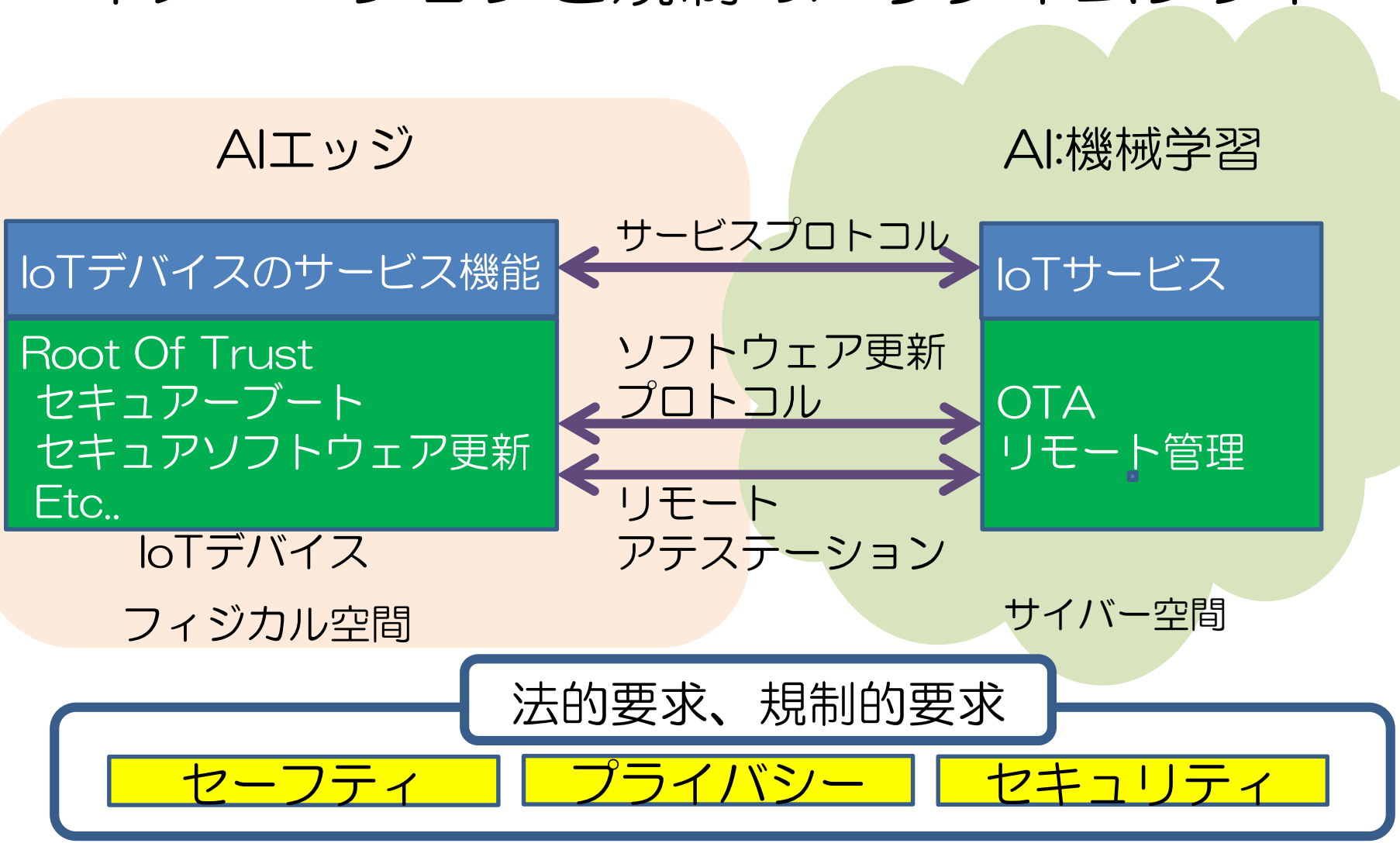


PKI day 2019
午前の部　IoTのトラスト

セコム IS研究所
Intelligent Systems Laboratory

- 講演「IoTにおけるトラスト実現に向けた技術的な仕組み」
  - 講師：株式会社レピダム　代表取締役
    菅野　　哲 氏
- 講演「セキュアなIoTを構築する技術
    -- Azure Sphere、Azure IoT Hubの場合」
  - 講師：日本マイクロソフト株式会社　エバンジェリスト
    太田　寛 氏
- 講演 「IoTセキュリティ強化のための技術戦略解説」
  - 講師：SHコンサルティング株式会社　代表取締役社長
    河崎　　俊平 氏
- 【パネルディスカション】「IoTのトラスト」

IoTのトラストが重要となっている背景
イノベーションと規制のパラダイムシフト



自動運転　修正に規制…
搭載プログラム　国が安全確認し許可　2019/02/04

出典：　https://www.yomiuri.co.jp/science/20190204-OYT1T50108/

- 国土交通省は、自動車メーカーが車に搭載されたシステムのプログラムを更新する場合、国の許可制とする方針を固めた。
- 今後、自動運転技術による高速道路での車線変更といったプログラムの更新が想定されるため、国が事前に安全性を確認できるようにする。
- 今年３月にも、開会中の通常国会に道路運送車両法の改正案を提出し、２０２０年の施行を目指す。→　通常国会で審議中

こうした規制案に対する辛辣な？？意見が？？

- そもそも自動車は、道路運送車両法(昭和26年法律第185号)により、型式認証を取得した車種に関して、個々の車が、OEMによる完成検査をへて、一般道道路の走行が許される。
- プログラム更新は、リコール制度（道路運送車両法第63条3）等との整合が必要になる。
- 「自動運転　修正に規制…」は、国連欧州経済委員会下の自動車基準調和世界フォーラム（WP29）で議論され→国内法へ

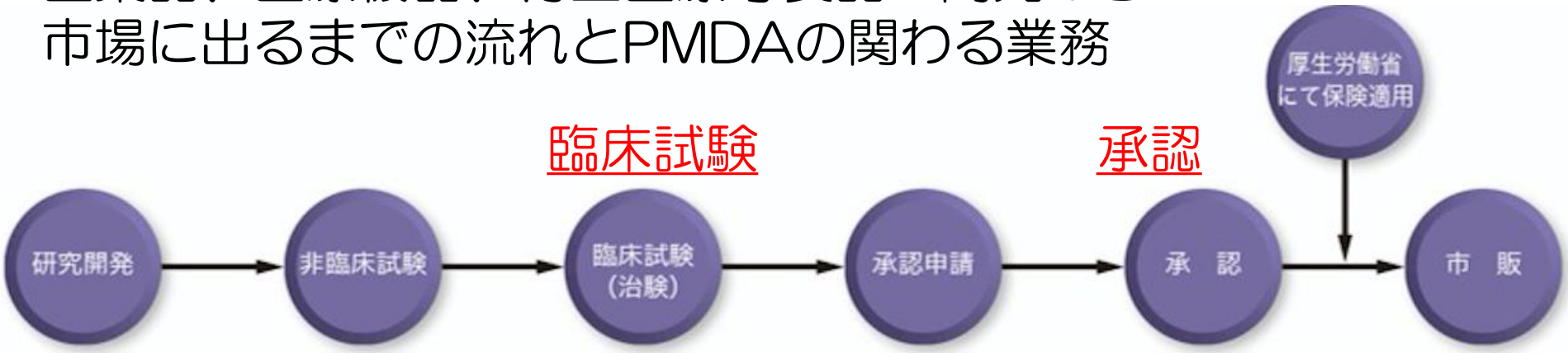
心電図をなぜ封印？Apple Watch Series 4 2018/09/25

出典 https://tech.nikkeibp.co.jp/atcl/nxt/column/18/00439/092000057/

- 2015年に登場した初代Apple Watch（中略）目玉は、画面の大型化と心拍センサー、心電図（ECG）機能であろう。なかでも心電図に注目した。現状（中略）近未来感にワクワクするではないか。だが、残念ながら日本発売のSeries 4では、心電図が封印されている。おそらく薬事法における、医療機器としての認証問題が絡んでいるのではないだろうか。

発売以降、心電図（ECG）機能により人命が助かったというニュースもそのたびに、規制に関しての批判が？？？

医薬品、医療機器、再生医療等製品の開発から
市場に出るまでの流れとPMDAの関わる業務



出典：独立行政法人医薬品医療機器総合機構（PMDA；Pharmaceuticals and Medical Devices Agency）
https://www.pmda.go.jp/review-services/outline/0001.html

米国食品医薬品局(FDA)の デジタルヘルスソフトウェア事前認証プログラム

セコムIS研究所 Intelligent Systems Laboratory

FDA U.S. FOOD & DRUG ADMINISTRATION

- “Software as a Medical Device” (SaMD)という考え方
- 従来からの「ハードウェアベースの医療デバイスを規制するためのFDAの伝統的なアプローチ」はSaMDの規制には、そぐわない。

Developing a Software Precertification Program:
A Working Model

v1.0 - January 2019

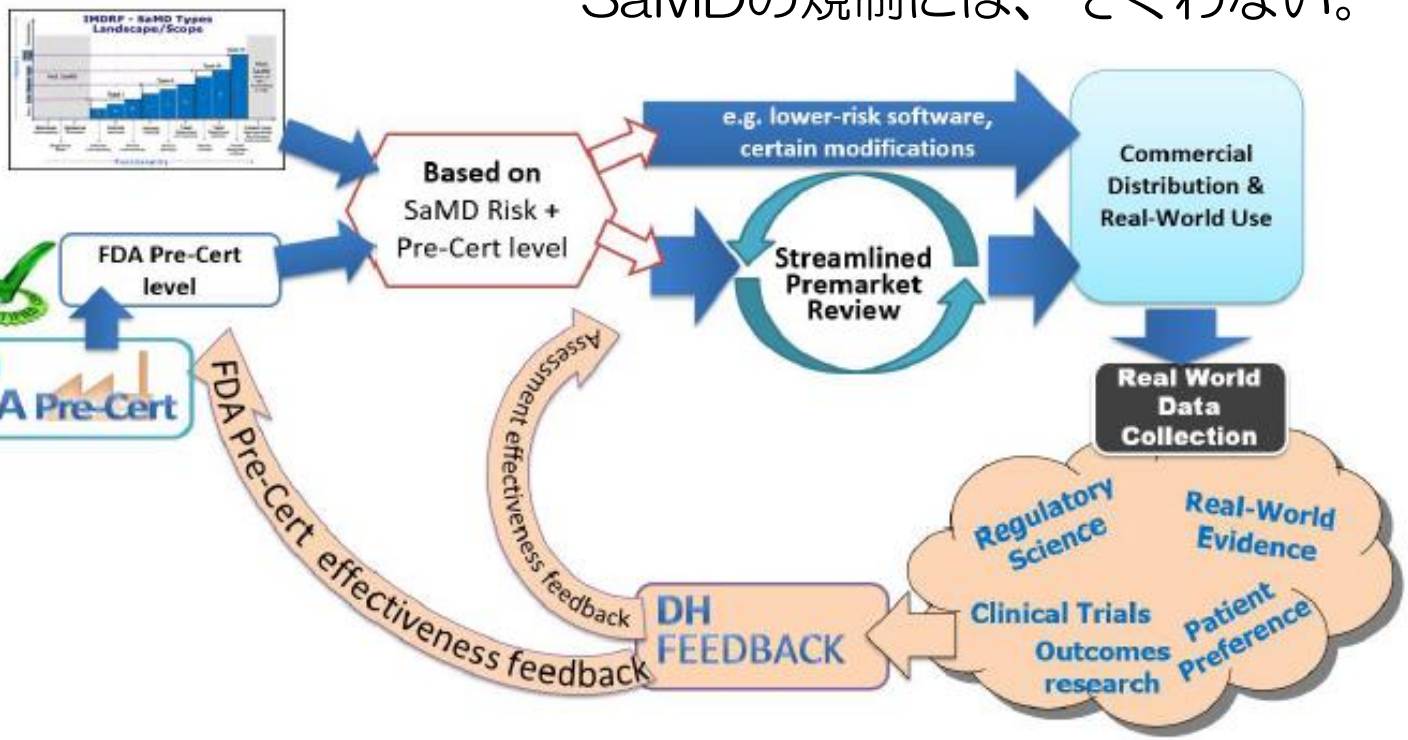


Figure 1. A reimagined approach for the regulation of software

出典:https://www.fda.gov/downloads/MedicalDevices/DigitalHealth/DigitalHealthPreCertProgram/UCM629276.pdf

デジタルヘルスソフトウェア事前認証プログラムとは

出典：https://globizz.net/fda_info/MD_info/pre_cert_program.html

セコムIS研究所 Intelligent Systems Laboratory

- 米国食品医薬品局(FDA)は、2017年7月に医療用ソフトウェア(Software as a Medical Device；SaMD)事前承認プロセスを構築するための、デジタルヘルスソフトウェア事前認証プログラム、Digital Health Software Precertification(Pre-Cert)Programを立ち上げ(中略)
- 《2017年7月に参加認定された企業９社》
  Apple社(米国)、Fitbit社(米国)、Johnson & Johnson社(米国)、Pear Therapeutics社(米国)、Phosphorus社(米国)、Roche社(米国)、Samsung Electronics社(米国)、Tidepool社(米国)、Verily社(米国)
- デジタルヘルスソフトウェア事前認証プログラムの特徴は、個々の製品ではなくその製品を手掛けている企業自体を事前に認証するところにあります。「製品」ではなく「企業」に焦点を当てている理由として、デジタルヘルスアプリなどの医療用ソフトウェアは機能の更新が随時行われることから、ソフトウェア製品ごとに有効性や安全性を審査していくことは非効率であるということが挙げられます。FDAが想定している事前審査とは、その企業のソフトウェア設計・検証・メンテナンスや企業としての透明性、リスク管理などについて審査し、優位性の高い企業であるかどうかをFDAが判断することです。また、サイバーセキュリティーにも重点が置かれています。

A Total Product Lifecycle Regulatory Approach for AI/ML-Based SaMD

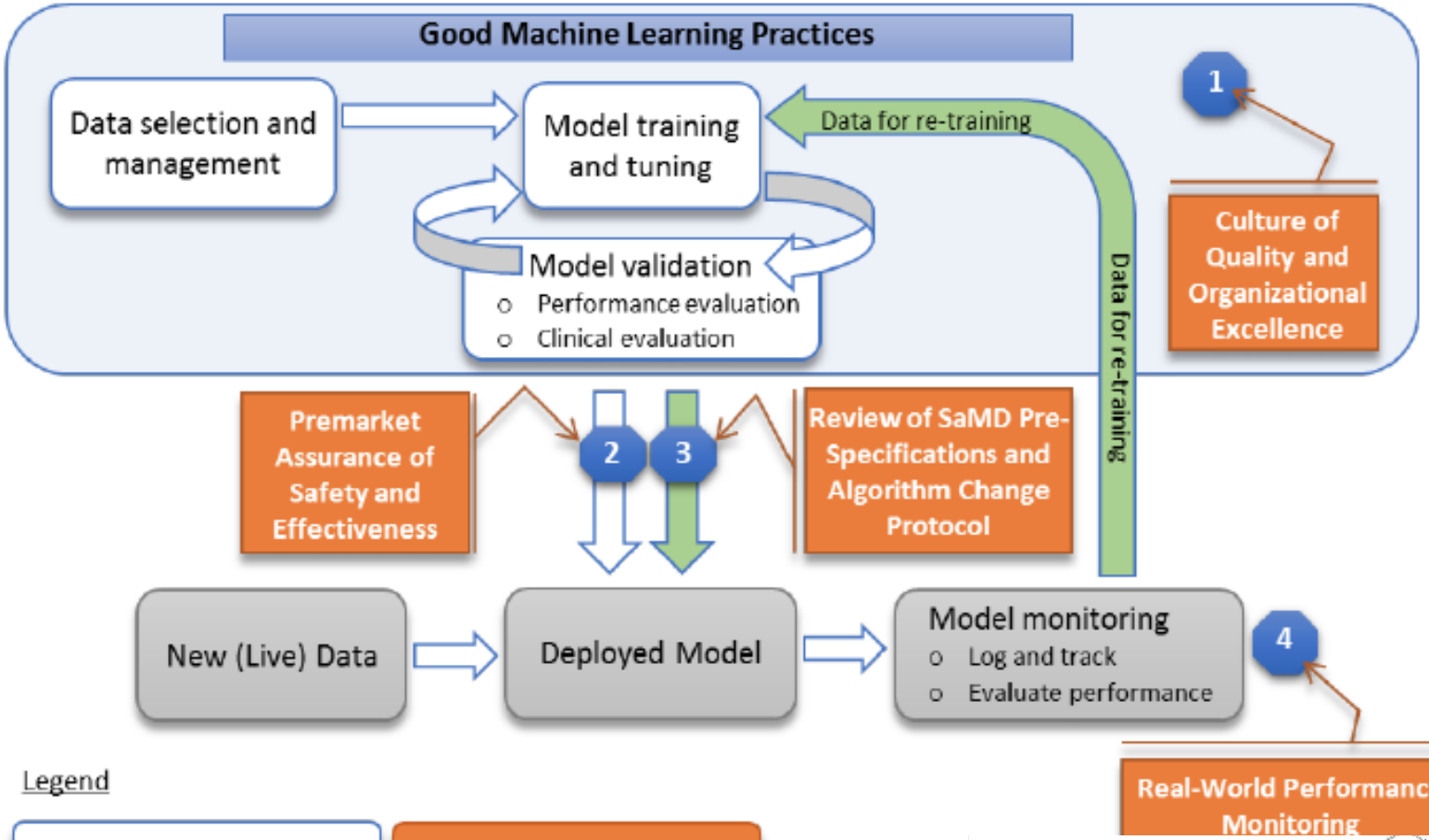
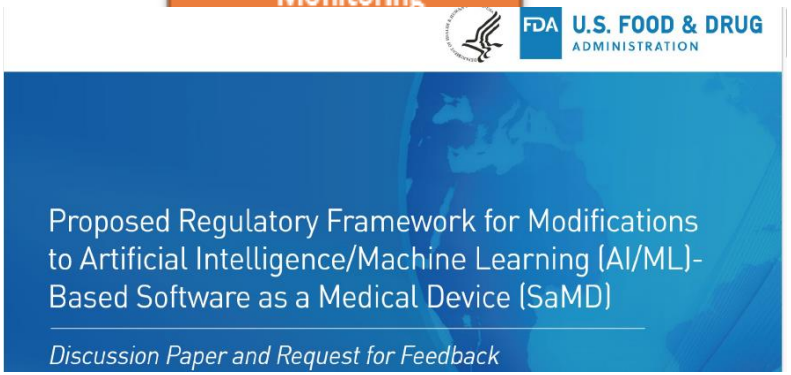


Figure 2: Overlay of FDA's TPLC approach on AI/ML workflow

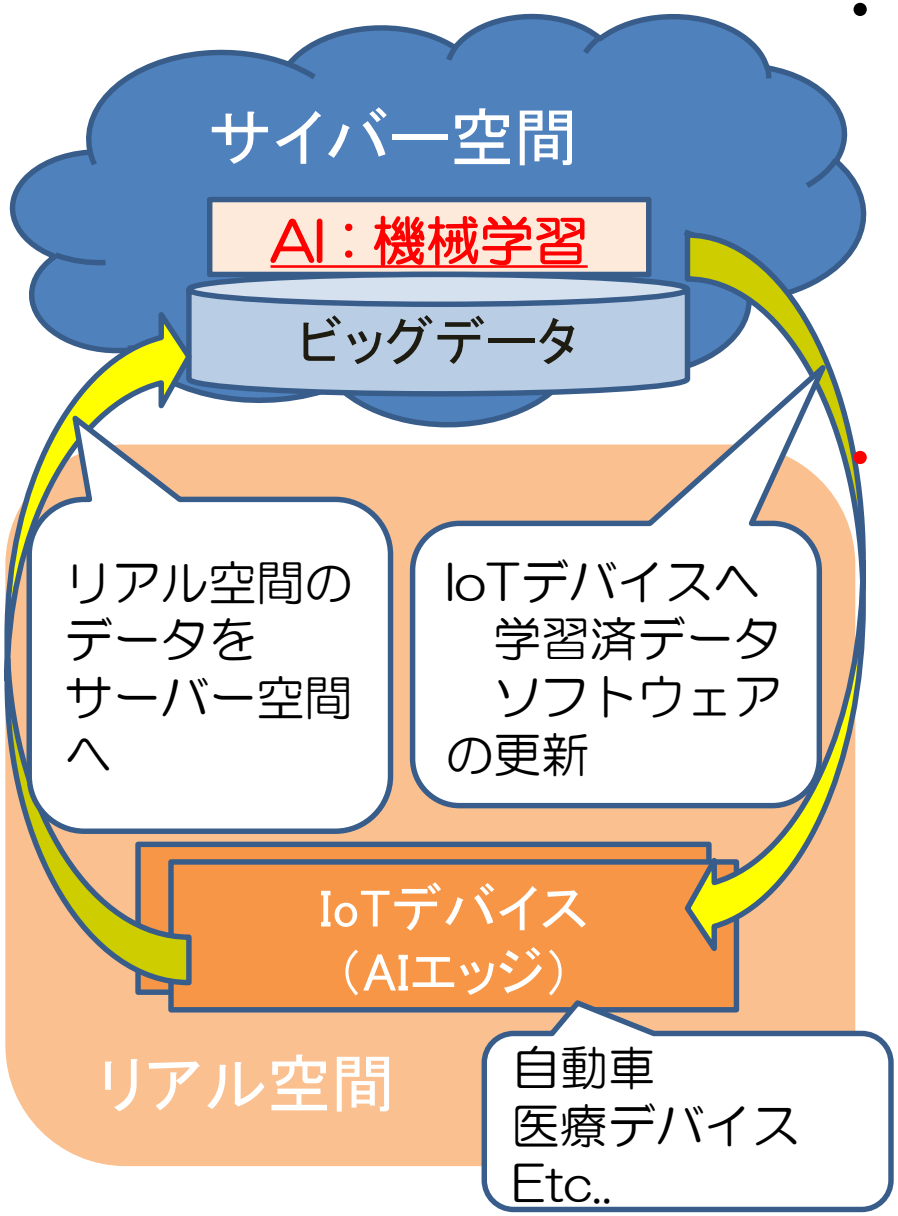
TPLC: Total Product LifeCycle



出典：https://www.fda.gov/downloads/MedicalDevices/DigitalHealth/SoftwareasaMedicalDevice/UCM635052.pdf

AI・IoTによるイノベーションと規制のパラダイムシフト

セコムIS研究所
Intelligent Systems Laboratory



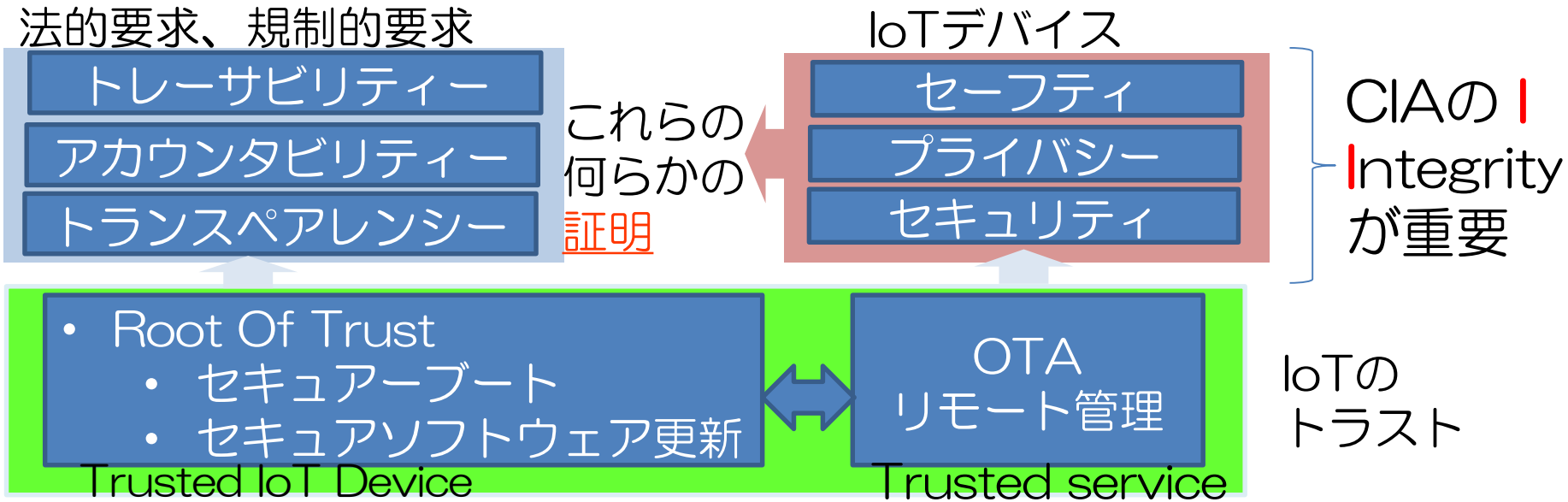
- AI・IoTによるイノベーション
  - 大量のIoTデバイスをリアル空間に配置し、大量のデータをサイバー空間に吸い上げ学習、その学習結果をIoTデバイス（AIエッジ）へ
  - IoTデバイス出荷後の改良と、新機能の追加などを実現
- 規制のパラダイムシフト
  - 製品（単体）の規制（従来の型式認証）からサービスシステムの規制へ
  - 製品出荷後の個別デバイスに対するトレーサビリティの要求
  - インシデント等に対するアカウンタビリティ
    - セーフティ（侵害）、プライバシー侵害、セキュリティ侵害
  - 高機能なIoTデバイス、複雑なサービスシステムに対するトランスペアレンシー

規制のパラダイムシフトに対応した「IoTのトラスト」

セコムIS研究所 Intelligent Systems Laboratory

- トレーサビリティ(traceability)
  - 出荷後の追跡、OTAによるリコール対応 →そのための個体識別（医療デバイスのUDI、自動車のVIN）とソフトウェアー更新の証跡管理など

  個体識別した上でのリモート管理、リモート・アテステーション
- アカウンタビリティ(accountability)
  - 事故時等のアカウンタビリティ-- ブレーキ問題めぐる集団訴訟とか
- トランスペアレンシー(transparency)
  - フォルクスワーゲン社による排出ガス不正事案 → ブラックボックス化



大量のIoTデバイスの管理（Integrity）を、暗号技術（主にデジタル署名技術）によりスケーラブル（スケールアウト）かつ効率的に実現。

セコムIS研究所
Intelligent Systems Laboratory

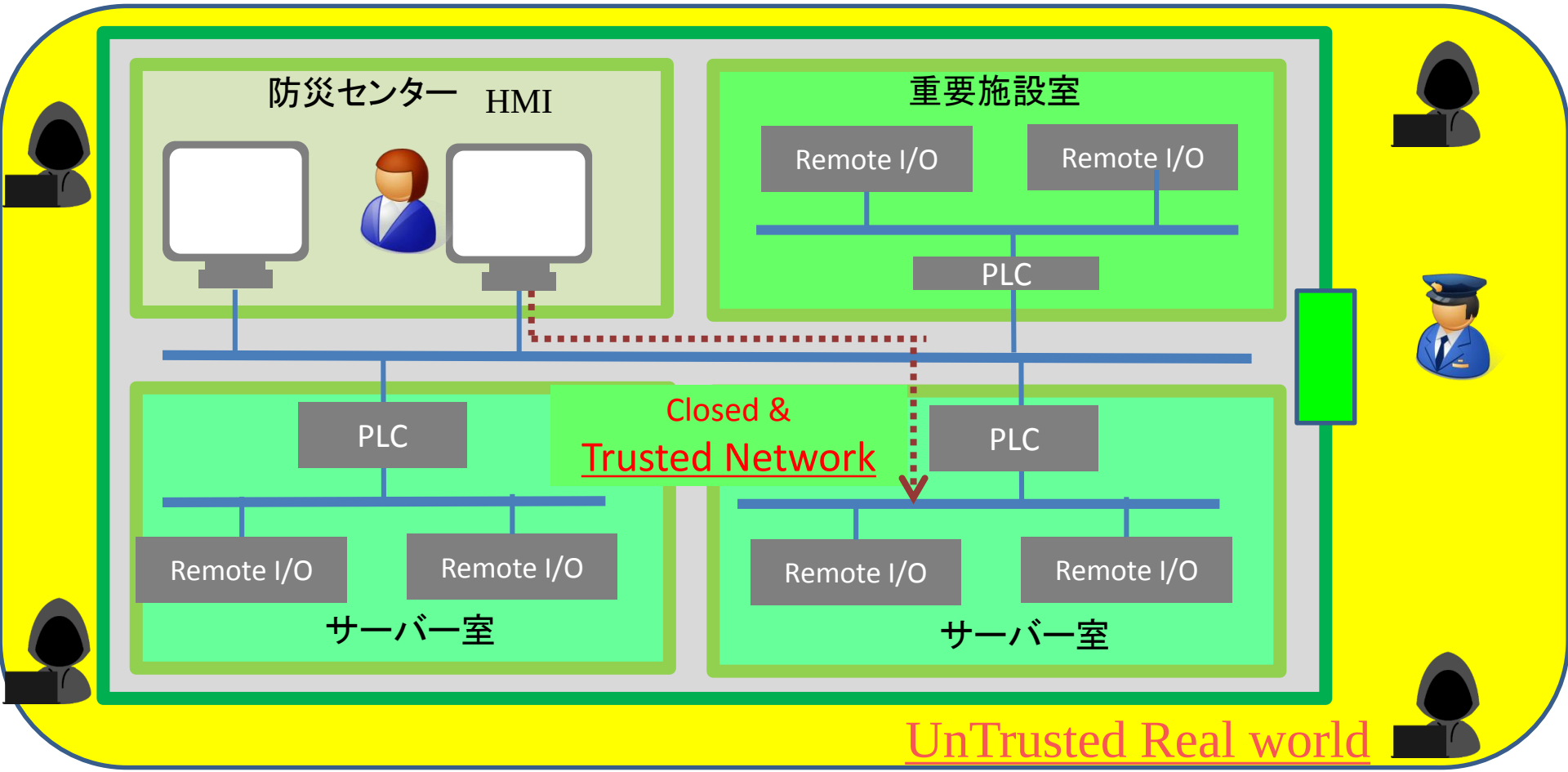
パネルディスカション
「IoTのトラスト」

菅野　哲 氏
　株式会社レピダム　代表取締役
太田　寛 氏
　日本マイクロソフト株式会社　エバンジェリスト
河崎　俊平 氏
　SHコンサルティング株式会社　代表取締役社長

重要インフラにおける物理セキュリティによるトラスト
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

セコムIS研究所
Intelligent Systems Laboratory

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続（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

空間　：　サイバー空間とフィジカル空間の融合
CPSにおけるIoTデバイスのトラスト

セコムIS研究所
Intelligent Systems Laboratory

Trusted IoT device＆暗号技術で構成された
フィジカル空間上のセキュリティ区画

時間軸：
IoTデバイスが生み出す価値とコスト
サービスの価値を支える「IoTデバイスのトラスト」

セコムIS研究所 Intelligent Systems Laboratory

サプライチェーンにおけるトラスト
トレーサビリティ、トランスペアレンシー、アカウンタビリティ

Society5.0型サプライチェーンセキュリティ

製造コスト　　サービスコスト

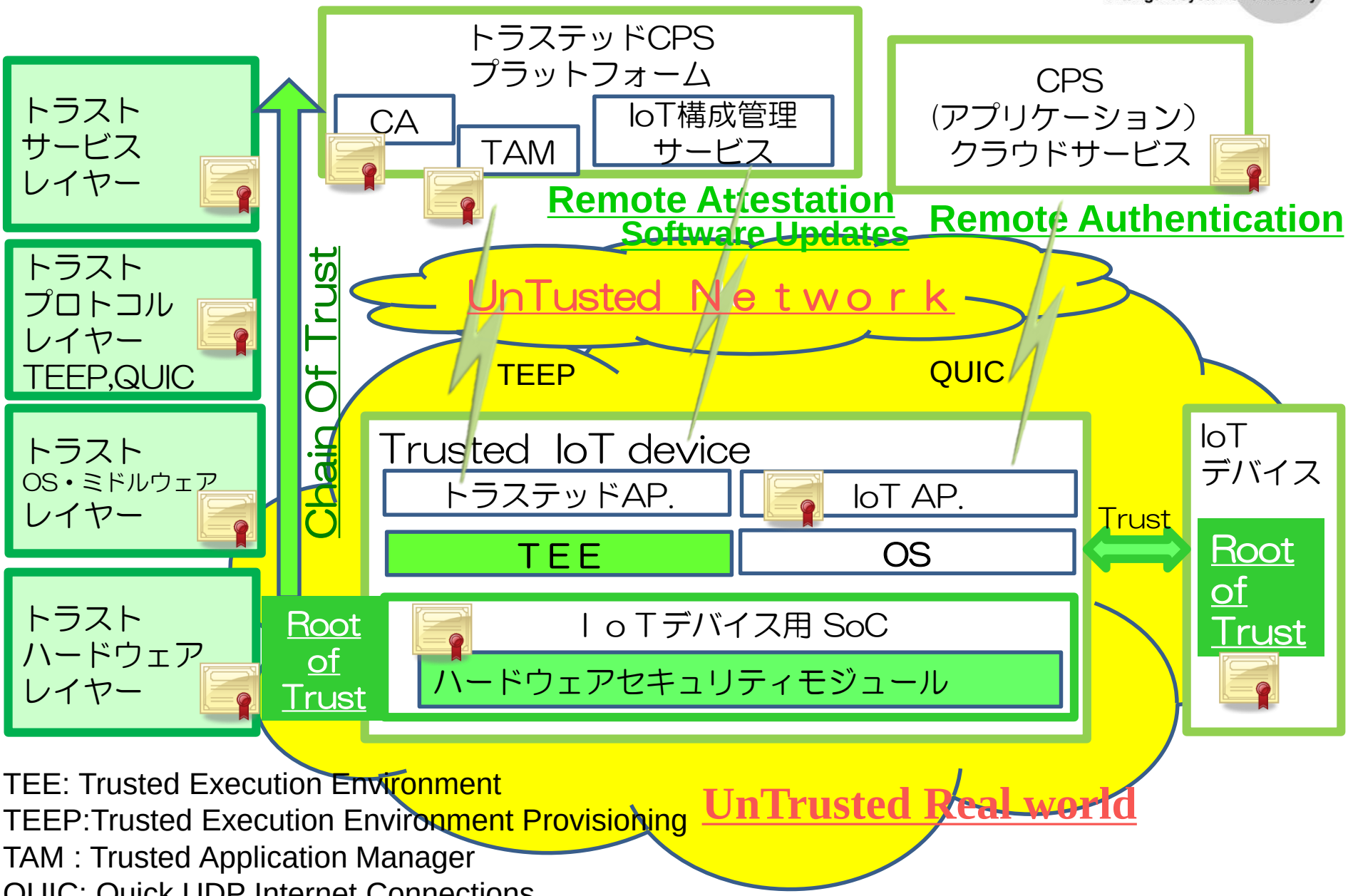
個別のIoTデバイスの観点
長期の暗号鍵管理に耐えうる
ハードウェアセキュリティ
HW Root of Trust（信頼の起点）

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

Trusted IoT device ⇒ トラストサービス

トラストなCPSのレイヤー構造

セコムIS研究所
Intelligent Systems Laboratory



TEE: Trusted Execution Environment
TEEP:Trusted Execution Environment Provisioning
TAM : Trusted Application Manager
QUIC: Quick UDP Internet Connections