PKI Day 2018

セコムIS研究所
Intelligent Systems Laboratory

超スマート社会（Society 5.0）におけるトラストの在り方

2018 年　4月　17日

松本　泰　　セコム（株）ＩＳ研究所

セコムIS研究所
Intelligent Systems Laboratory

超スマート社会（Society 5.0）における トラストの在り方

- (1) PKI day 2018 オーバービュー
- (2) パネルディスカション
- 付録
  - 自動車における暗号技術によるトラスト
  - 暗号技術とサービスイノベーション
  - 過去のPKI day の参考スライド

PKI day 2018 までの歩み

セコムIS研究所

回	年	PKI day テーマ	
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	

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

セコムIS研究所 Intelligent Systems Laboratory

- 我が国の施策として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、社会の効率化が目指された社会と言えます。
- この時、膨大な数のIoTデバイス等が「繋がることによる新しい価値の創造」のためには、何らかの信頼と信頼関係の構築、すなわちトラストの構築が必要になります。
- このトラストの構築に欠かせない技術が、暗号技術／公開鍵暗号技術、そしてPKIだと言えます。
- PKI day 2018では、以上を踏まえ「超スマート社会（Society 5.0）におけるトラストのあり方」をテーマに、今後の社会において暗号技術／公開鍵暗号技術／PKIが果たすべき役割を議論します。

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

セコムIS研究所
Intelligent Systems Laboratory

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）

超スマート社会におけるIoT/BD/AI

セコムIS研究所 Intelligent Systems Laboratory

- 非常に低コストで、かつ高機能なコモディティ化したIoTデバイス
  - このIoTデバイスを最大限に利活用
- サイバー空間とフィジカル空間が高度に融合 ≒ CPS（Cyber Physical Systems）
  - 大量のIoTデバイスをフィジカル空間に配置
    - IoTデバイス（センサー、アクチュエータ）
  - フィジカル空間のデータをサイバー空間へ　（ビッグデータ）
  - サイバー空間上で、AI等による学習、判断等の処理
  - 判断結果等をフィジカル空間へIoTデバイス等を介して反映
- 多様なステークホルダー・エンティティを繋げることによる価値の創造
  - Soecity5.0・第４次産業革命におけるサービスイノベーションへ

⇒この時、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セキュリティは、どのような考えるべきなのか？
　CPS（Cyber Physical Systems）のためのセキュリティ

超スマート社会における
セキュリティ・プライバシー・トラスト(IoTを中心に)

セコムIS研究所 Intelligent Systems Laboratory

脆弱性対応としての セキュリティ対策

- IoTデバイスのライフサイクルを考慮したセキュリティ・バイ・デザイン
- インシデント情報の収集
- マルウェア解析
- Etc..

プライバシー保護

- IoT利活用のためのプライバシー・バイ・デザイン
- 個人情報の利活用と保護を両立するためのプライバシー保護技術
- Etc..

暗号技術によるトラスト

- IoTデバイスへの暗号技術の組み込み
- ハードウェアセキュリティ(Hardware Root of Trust)の組み込み
- 大量の暗号鍵管理
- Etc..

- セキュリティ対策　⇒　悪意ある第3者からの攻撃を防ぐ
- トラストの観点 ⇒　ステークホルダー・エンティティの信頼関係の構築
  - 「繋げることによる価値の創造」　IoTデバイスのビューからは、
    - 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？

価値の創造のためには、Trust by designが必要であり
暗号技術によるトラストが重要な役割を果たす

自動車のCASE化から見た セキュリティ・プライバシー・トラスト

セコムIS研究所 Intelligent Systems Laboratory

（表向きの）車の新たな役割、機能

車のCASE化？？？

- Connected コネクテッド
- Autonomous 自動運転
- Shared & Services
- Electric 電動化

非機能要件？？？

誰がコスト負担？？？

CASE化を支えるCybersecurity

- Security
- Safety
- Privacy
- Trust

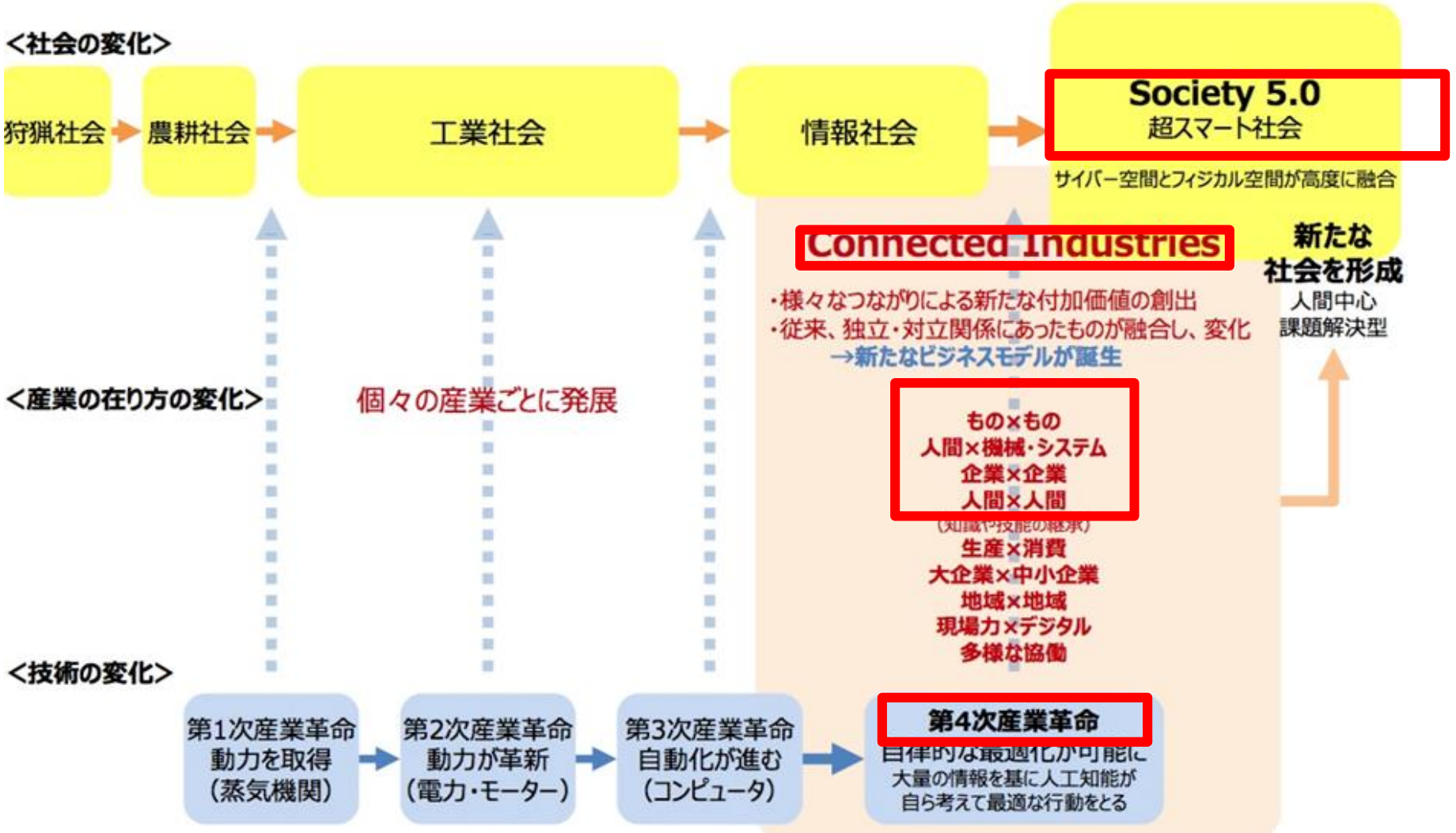
既存の製造業的観点が強い

車の価値がサービスに移行した場合には、サービスモデル・ビジネスモデルの依存性が大きい。
Privacy, Trustは、ビジネスデザインでもある

参考　→　付録：自動車における暗号技術によるトラスト

社会の変化に伴うトラストの概念の変化（１）

セコムIS研究所 Intelligent Systems Laboratory



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）

セコムIS研究所
Intelligent Systems Laboratory

- 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

セコムIS研究所 Intelligent Systems Laboratory

- 「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

参考　->　付録：暗号技術とサービスイノベーション

超スマート社会におけるトラストの課題

セコム IS研究所 Intelligent Systems Laboratory

- 技術
  - IoTデバイス等における暗号技術の要求
    - ハードウェアセキュリティ
    - 様々なトレードオフが必要な環境下での公開鍵暗号技術の実装
  - 公開鍵暗号の長期的なセキュリティ、マイグレーション
  - Etc…
- 法制度
  - クロスボーダー（業界、地域）
  - 法制度との整合、ポリシーの整合
  - Etc..
- ビジネス、産業競争力、サプライチェーンリスク、etc…
  - マルチステークホルダー、エコシステムとトラスト
  - 競争の中でのトラスト
  - Etc..

PKI day 2018 プログラム　午前の部

セコム IS研究所 Intelligent Systems Laboratory

- 10：00 - 10：20
  - 【ご挨拶】「PKI day 2018のオーバビュー」
  - セコム株式会社 IS研究所／PKI相互運用技術WGリーダー　松本 泰 氏
- 10：20 - 11：10
  - 【基調講演】「トラストとトラストレスの狭間で」
  - 講師：京都大学 公共政策大学院 教授　岩下 直行 氏
- 11：10 - 11：50
  - 【講演】「量子コンピュータ時代の公開鍵暗号」
  - 講師：セコム株式会社 IS研究所　伊藤 忠彦 氏
- 11：50 - 12：30
  - 【講演】「before ROCA / after ROCA / beyond ROCA から見えてくるRSA暗号実装の闇」
  - 講師：株式会社インターネットイニシアティブ 須賀 祐治氏

PKI day 2018 プログラム　午後の部

セコムIS研究所
Intelligent Systems Laboratory

- 13:30 – 14:10
  - 【講演】「Androidのコード署名に学ぶIoT時代のソフトウェアアップデート」
  - 講師：東邦大学理学部　准教授 金岡　晃 氏
- 14:10 – 15:00
  - 【講演】「PKIが熱望される場＝繋がるクルマ」
  - --具体的なユースケース、そこで生まれる恩恵と脅威、それらへの方策―
  - 講師：富士通株式会社 Mobility IoT事業本部 小谷 誠剛 氏
- 15:00 – 15:20
  - 休憩
- 15:20 – 17:40
  - 【パネルディスカション】
  - 「超スマート社会（Society 5.0）におけるトラストの在り方」

PKI day 2018のプログラムの意図

セコムIS研究所
Intelligent Systems Laboratory

- 超スマート社会への変化
  - 金融・Fintech　⇒　「トラストとトラストレスの狭間で」
  - 自動車　⇒　「PKIが熱望される場＝繋がるクルマ」
- 超スマート社会は、暗号技術・公開鍵暗号技術に大きく依存する社会
  - ⇒「量子コンピュータ時代の公開鍵暗号」
  - ⇒ 「Androidのコード署名に学ぶIoT時代のソフトウェアアップデート」
  - ⇒ 「before ROCA / after ROCA / beyond ROCA から見えてくるRSA暗号実装の闇」
- 超スマート社会におけるトラストに係る技術・法制度・ビジネスの関係
  - ⇒　パネルディスカション

パネルディスカション
超スマート社会（Society 5.0）
におけるトラストの在り方

超スマート社会（Society 5.0）におけるトラストの在り方 パネリスト

セコム IS研究所 Intelligent Systems Laboratory

- 石原 修 氏
  - COCN 2017年度推進テーマ「Society5.0を支えるセキュアトラスト基盤」リーダー
  - 株式会社日立製作所　セキュリティ事業統括本部　担当本部長
- 山内 徹 氏
  - 一般財団法人日本情報経済社会推進協会 常務理事 インターネットトラストセンター長
- 宮崎 一哉 氏
  - タイムビジネス協議会副会長（トラストサービス推進フォーラム）
  - 三菱電機株式会社
- 小川 博久 氏
  - JNSA電子署名WGサブリーダー（日本トラストテクノロジー協議会）
- 小谷 誠剛氏
  - TCG常任理事
  - 富士通株式会社

ディスカッション

セコムIS研究所
Intelligent Systems Laboratory

- お題目その１
  - セキュリティとトラストの関係、セキュリティとトラストの違い
  - そもそもの「トラスト」の定義
  - なぜ、「トラスト」をキーワードとして取り上げているのか？
  - 超スマート社会において、何が証明できるのか、何を証明するべきなのか？
- お題目その２
  - クロスボーダ対応、グローバル対応をどう考えるのか
  - 過去の法制度からのオーソリティの違い（電子署名とタイムスタンプ）
- お題目その３
  - トラストに関する技術的課題、制度的課題、ビジネスとの関係

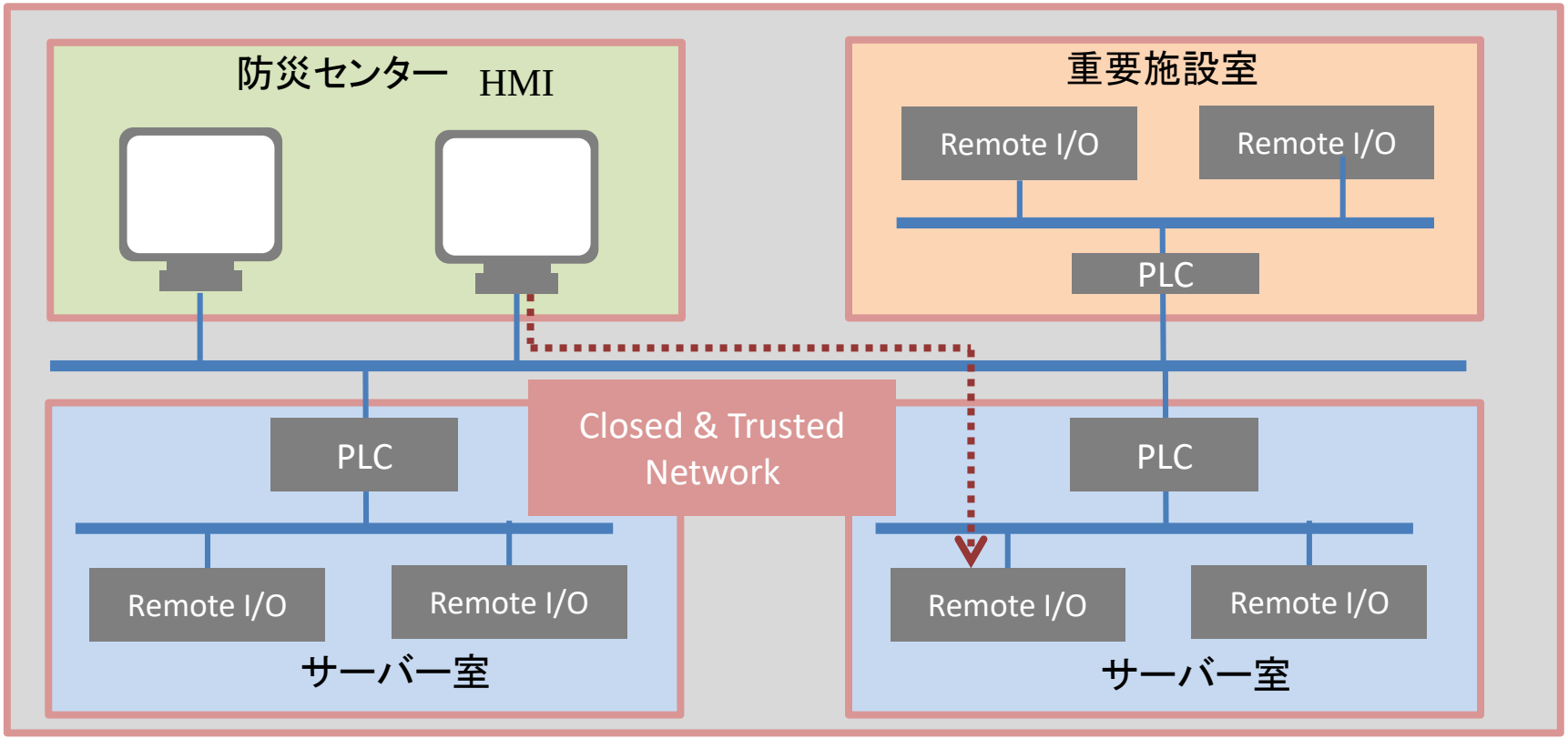
セコムIS研究所
Intelligent Systems Laboratory

暗号技術とサービスイノベーション

（現状の）重要インフラ・制御システムのセキュリティ

セコムIS研究所 Intelligent Systems Laboratory

物理的なゾーニングと物理鍵管理等によるアクセス制御でセキュリティを確保
⇒　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

（現状の）サイバー空間のセキュリティ
物理的環境+暗号技術で「トラスト」を確保

セコムIS研究所
Intelligent Systems Laboratory

ビジネスレイヤーでは…

インターネット上で、人とサービスの
トラストを構築したい

サービス

物理的環境 ＋ 暗号技術でセキュリティを担保

Trusted

PC内の
Root証明書

脳の中の
弱いパスワード

家（弱い物理セキュリティ）

UnTrusted

認証・
暗号化通信

暗号鍵の関係がトラストを構築、
利用者はサービスを信頼する

Trusted

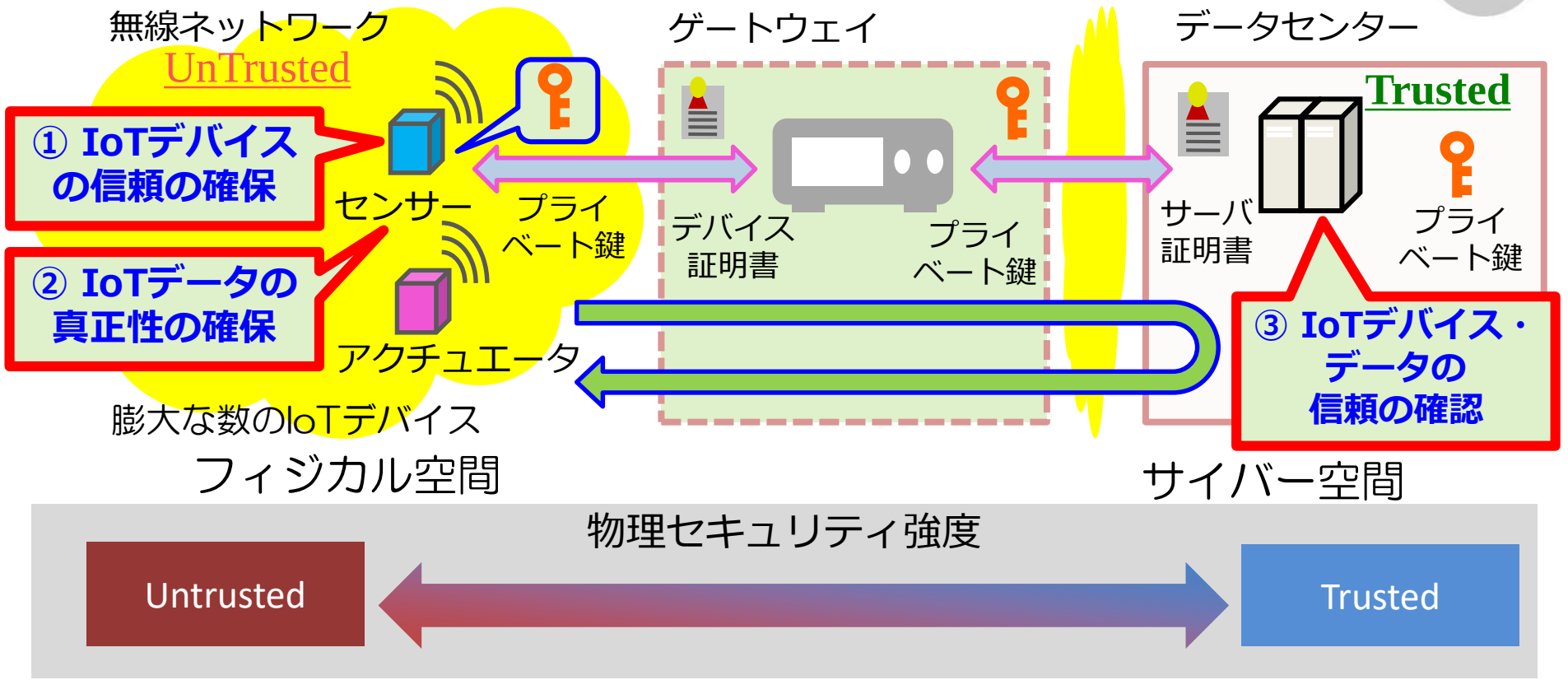
Web証明書の公
開鍵に対応する
プライベート鍵

データセンター（強い物理セキュリティ）

Untrustedなインターネットを介してTrustを確立するのがトラストテクノロジの一つの目標だった。

空間：
フィジカル空間とサイバー空間が高度に連携した社会

セコムIS研究所 Intelligent Systems Laboratory



- IoTデバイスの信頼、IoTデータの真正性の確保に加えてつながる先での「**確認**」も必要
- IoTデバイスは弱い物理的環境に置かれることが想定されるため、物理的環境による保護に代わる「**ハードウェアセキュリティ**」が重要となる

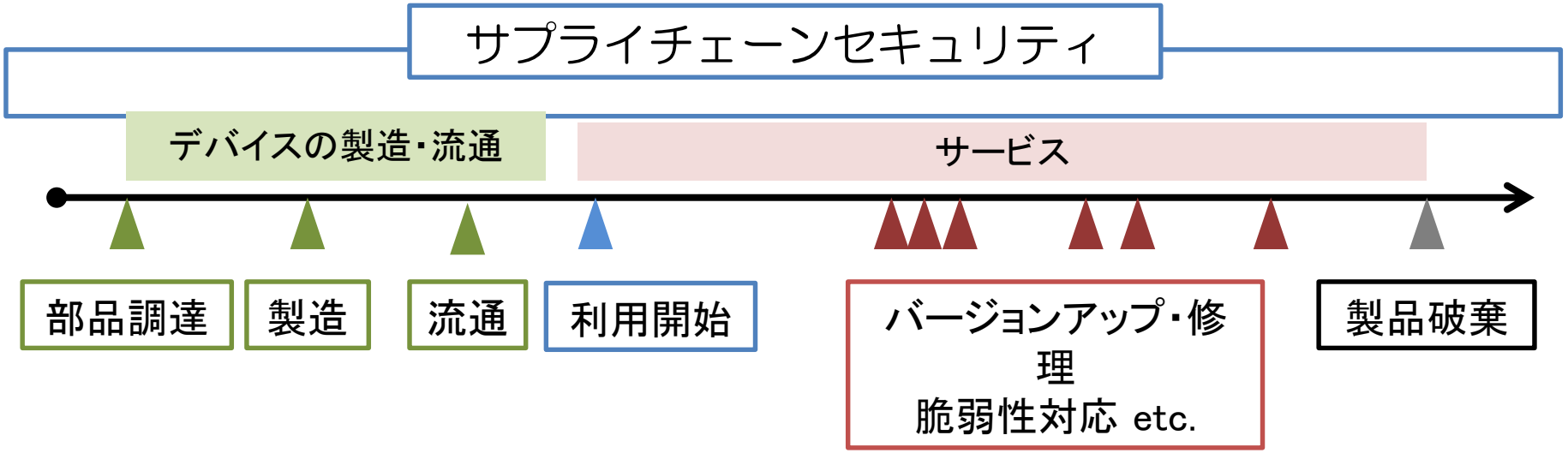
⇒　IoTセキュリティが確保されていることを“つながる相手”と確認し合うために

フィジカル空間のIoTデバイスも含めた「暗号技術によるトラスト」が重要

時間軸：
IoTデバイスが生み出す価値・コスト・セキュリティ

セコム IS研究所 Intelligent Systems Laboratory

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

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

セコムIS研究所
Intelligent Systems Laboratory

自動車における暗号技術によるトラスト

車における「暗号技術によるトラスト」の要求

セコムIS研究所 Intelligent Systems Laboratory

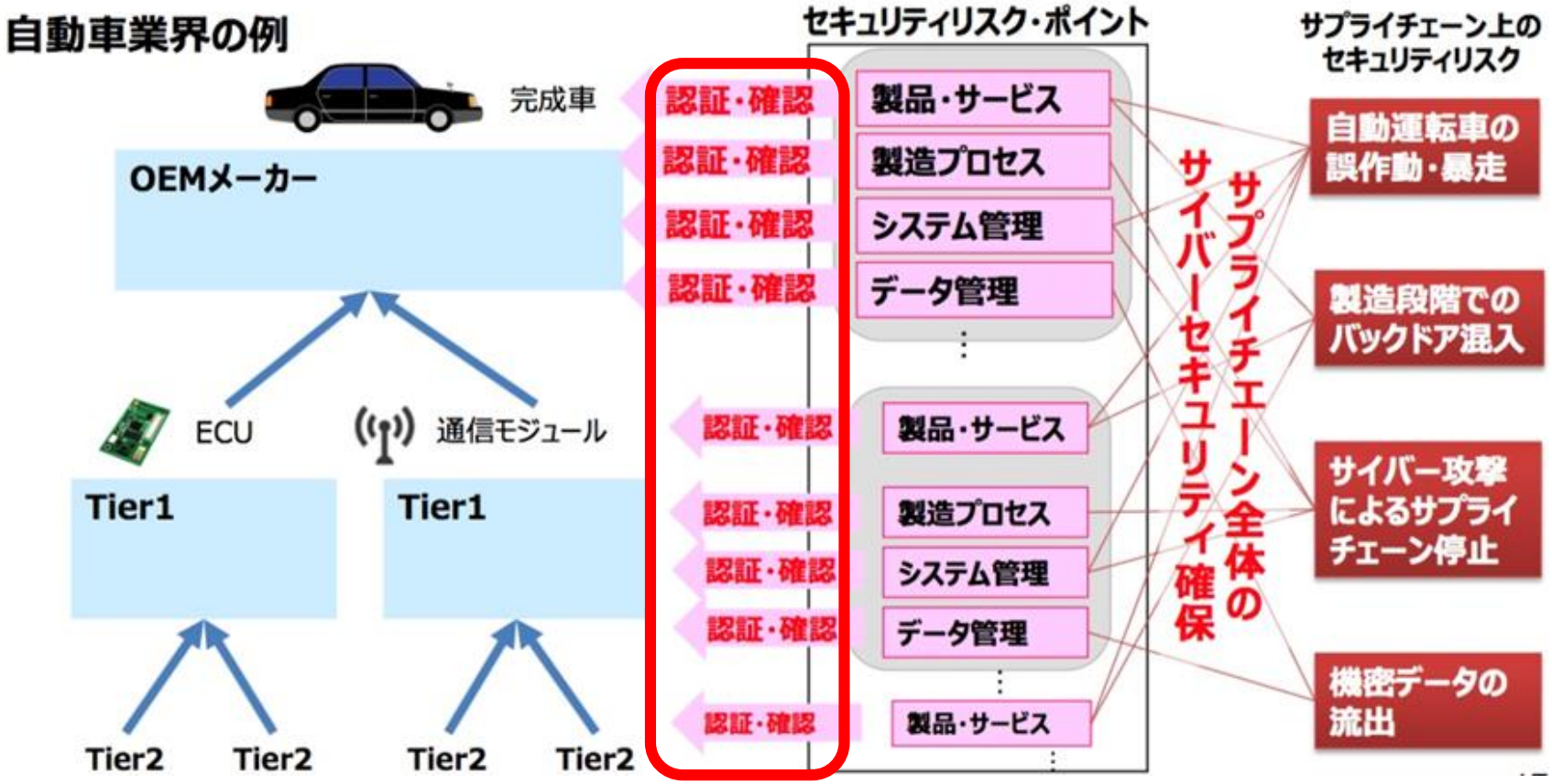
- 現在進行中、検討中の車における暗号技術によるトラスト
  - ECUに組み込まれるSHE（Secure Hardware Extension）-- ECU間のトラスト
  - 車車間通信、路車間通信　（ITS）
  - 高度化・複雑化するソフトウェアの更新（OTA）

サプライチェーン全体の対策強化
–サイバーセキュリティ対策フレームワークの策定–

セコムIS研究所 Intelligent Systems Laboratory

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

- サプライチェーン全体のセキュリティリスク・ポイントを明らかにし、リスク評価手法や認証・確認方法を定めた「サプライチェーン対策フレームワーク」の策定を検討。



暗号技術によるトラストの期待される役割の一つは、サブライチェーンにおける「確認」やSupply Chain Integrityを最小限の人的リソースで実現すること

欧州のR&Dプロジェクトの比較

セコムIS研究所
Intelligent Systems Laboratory

	Evita	SimTD	Oversee	Preserve	ISE
Start date	2008 - 2011	2008-2013	2010 - 2012	2011 - 2015	2014 - present
Real testbeds	X			X	X
Simulations		X		X	X
Evaluation of security	X			X	X
Evaluation of privacy	X			X	X
Inter-vehicle security	X	X	X	X	X
Intra-vehicle security	X				
Reuse of existing project components			X	X	
Use of real PKI				X	X

Table 2 - Qualitative comparison of the security projects

- Evita Prj.の成果のIntra-vehicle security が、SHE（Secure Hardware Extension）として、ECUに組み込まれつつある。
- Preserve　Prj.の成果であるInter-vehicle　security として、欧州のITS-C等の実証実験を経てPKI（公開鍵基盤）の構築と車への組み込み等が本格する？？

出典：An Overview of Security Ongoing Work in Cooperative ITS
https://hal.archives-ouvertes.fr/hal-01618760/document

2018年3月16日のニュース

セコムIS研究所
Intelligent Systems Laboratory

- ［特報］トヨタ、19年に電子基盤刷新　全車に暗号導入
  - 2018/03/16
  - 清水 直茂＝日経 xTECH／日経Automotive
  - 出典：http://tech.nikkeibp.co.jp/atcl/nxt/column/18/00001/00185/
  - トヨタ自動車が、2019年に発売する車両から電子プラットフォーム（基盤）を刷新することが日経 xTECH／日経Automotiveの取材で分かった。グループのほぼ全車両が対象。自動運転技術の本格導入に備える。通信データ量の増大に対応することに加えて、ハッカーによる車への攻撃を防ぐ。
- ［特報］ホンダも車に暗号、トヨタと同年量産
  - 2018/03/16
  - 清水 直茂＝日経 xTECH／日経Automotive
  - 出典：http://tech.nikkeibp.co.jp/atcl/nxt/column/18/00001/00162/
  - ホンダが、2019年に量産する車両から暗号技術を採用する。ハッカーによる車の乗っ取りを防ぐ。トヨタも、同年から量産車に暗号技術を搭載する。“つながるクルマ”の普及をにらみ、日本の自動車産業全体を巻き込んだ車のハッカー対策が始まる。

マルチステークホルダー下での暗号鍵管理
ECUに係るステークホルダーと権限管理

セコムIS研究所
Intelligent Systems Laboratory

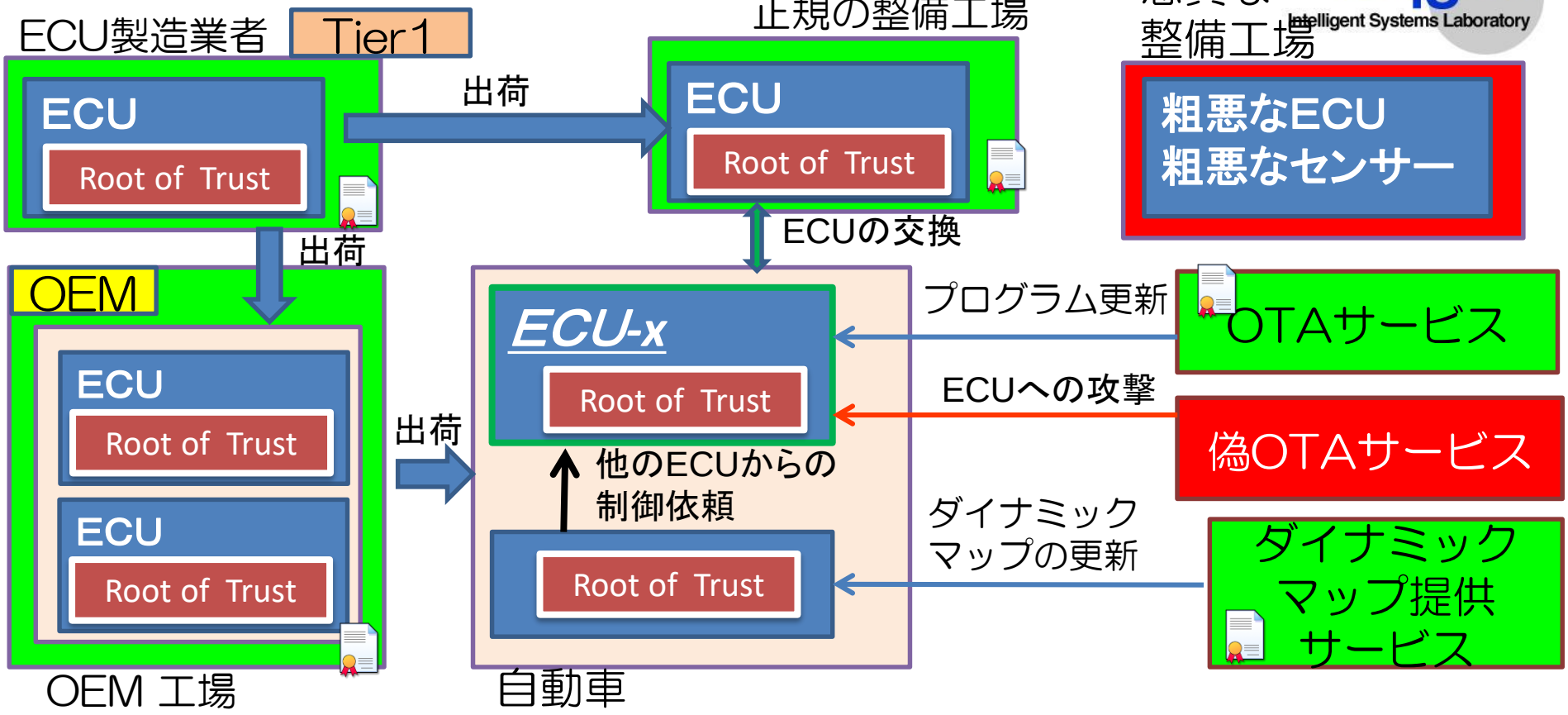
番号	ロール	権限レベル	権限
ユーザロール1	ECU製造者	高い	ECU自体へのアクセスとアップデート
ユーザロール2	自動車メーカー		各装置へのアクセスとアップデート
ユーザロール3	修理工場		自動車メーカーから配布されたツールをもとに各装置へのアクセスとアップデート
ユーザロール4	検査機関/警察		OBDポートから各装置の状態の読み込み
ユーザロール5	オーナー/運転手	低い	アクセス権なし

Horizon 2020 Program, SHARCS(Secure Hardware-Software Architectures for Robust Computing Systems), Deliverable D2.1, “SHARCS Applications and framework requirements for secure-by-design systems”から抜粋・訳

- こうした、マルチステークホルダーによる権限管理の理想モデルとして、PKI（公開鍵基盤）による各エンティティを証明する公開鍵証明書と、証明された各エンティティの権限を証明する属性証明書を使うモデルがある。
- しかし、すべてのECUにおいて公開鍵を扱うことは難しく、公開鍵と共通鍵のハイブリッドモデルを考える必要がある　→これが簡単ではない！！

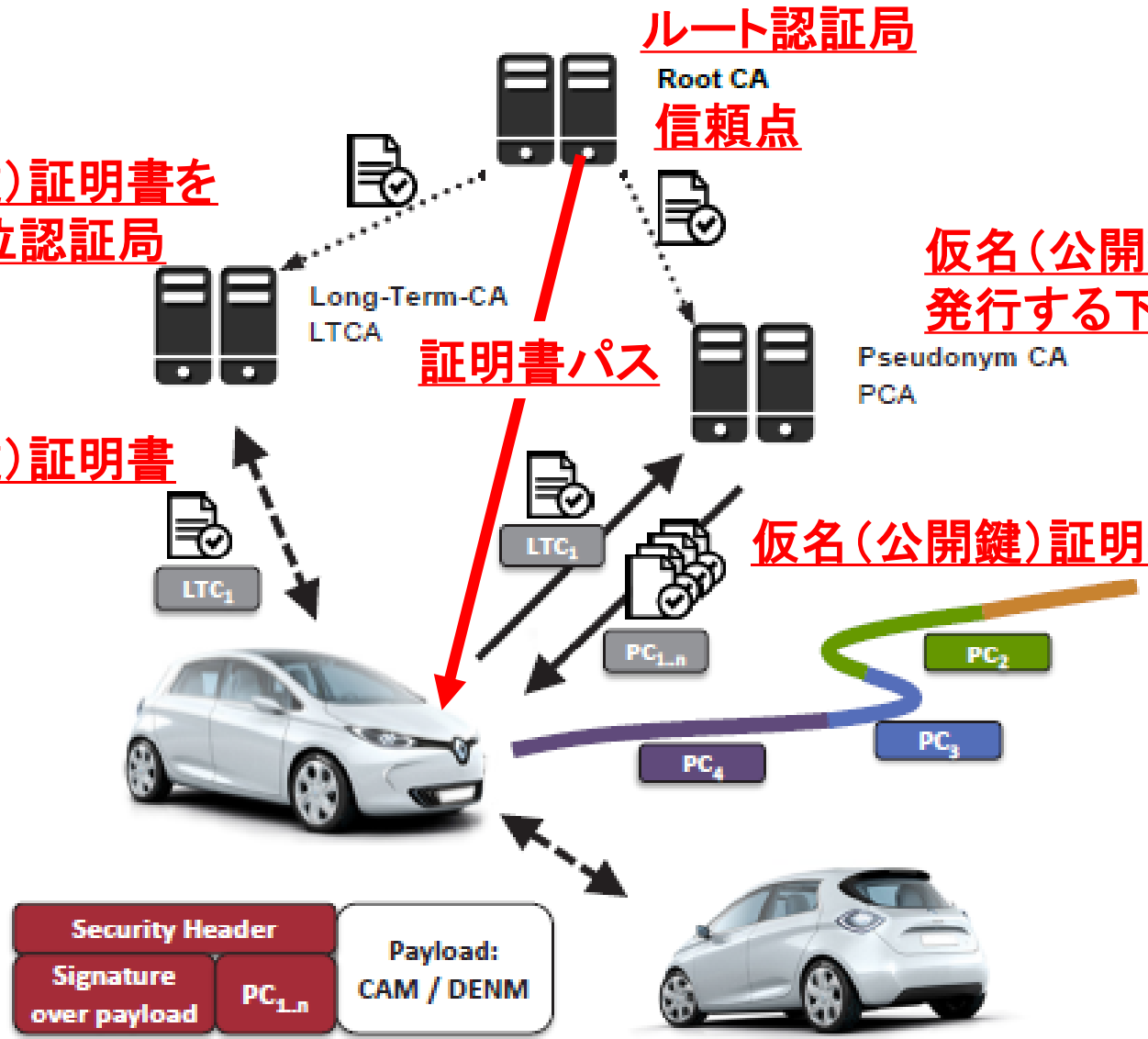
理想的には、ＥＣＵの(アクセス制御のための）自律性が重要(そのためのRoot of Trust 、ハードウェアーセキュリティ、公開鍵暗号基盤(PKI)、暗号鍵管理)

ECUのアクセス制御のToBE



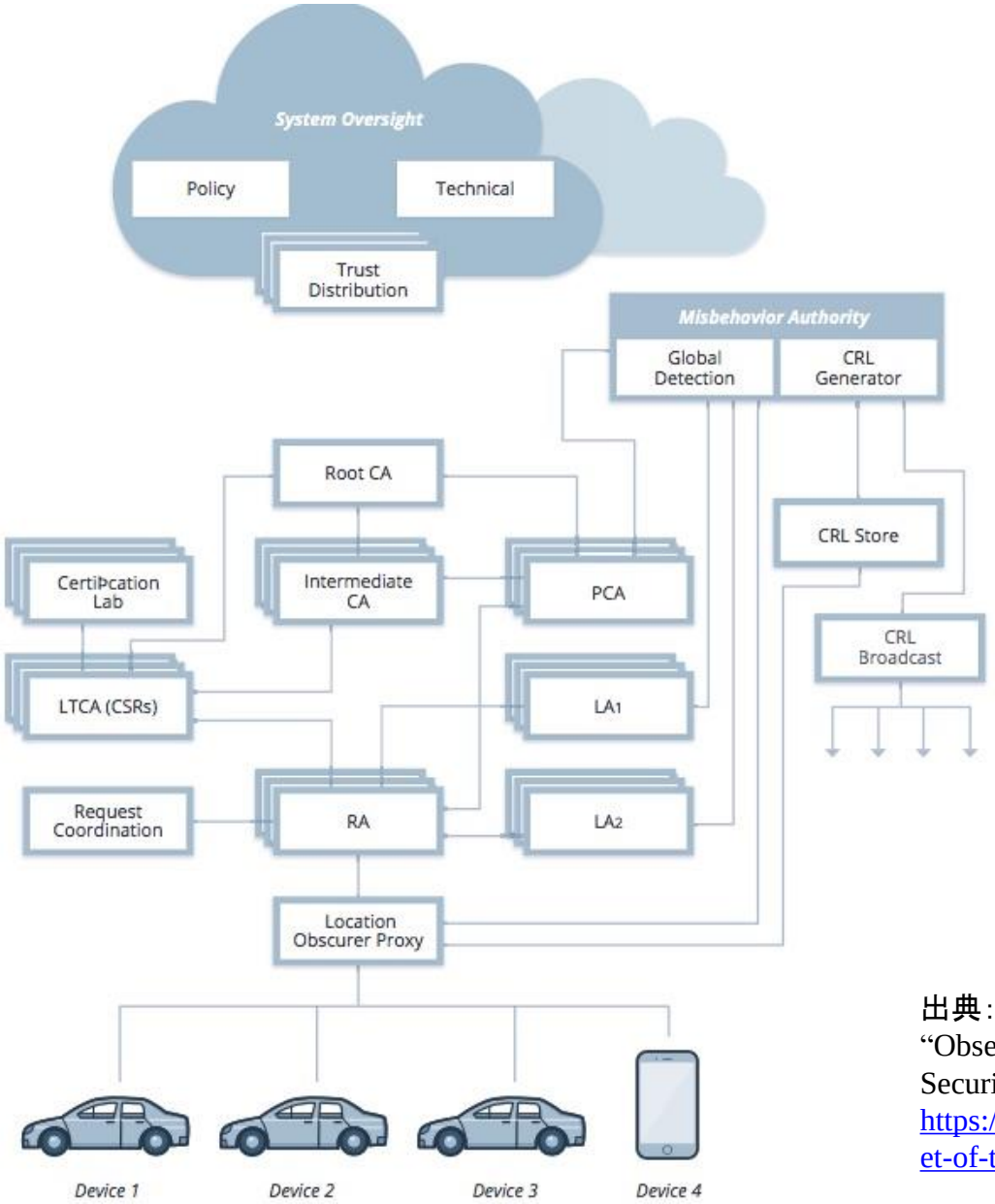
- ECU-xへのプログラム更新を含む、様々なステークホルダーからのアクセス
- ECU-xのアクセス制御のToBeは、自分自身に組み込まれたRoot of Trust のみを信頼し、正当な機関からの権限付与のデジタル署名を検証すること。

欧州FP7 PRESERVE(2011-2015)における実証実験



出典:http://staff.cs.kyushu-u.ac.jp/data/event/2015/02/150708_Dennis%20Kengo%20Oka.pdf

USDOT（米国運輸省）が主導するSafety Pilotプロジェクト SCMS（Security Credential Management System）



2017年に３つの地区での実証実験
Connected Vehicle Pilot Deployment Program
https://www.its.dot.gov/pilots/index.htm

- New York City (NYC) DOT Pilot
- Tampa (THEA) Pilot
- Wyoming (WY) DOT Pilot

出典:
“Observations and Recommendations on Connected Vehicle Security” By Cloud Security Alliance (CSA)
https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/connected-vehicle-security.pdf

欧州のITS-Cにおける証明書発行と証明書ポリシー

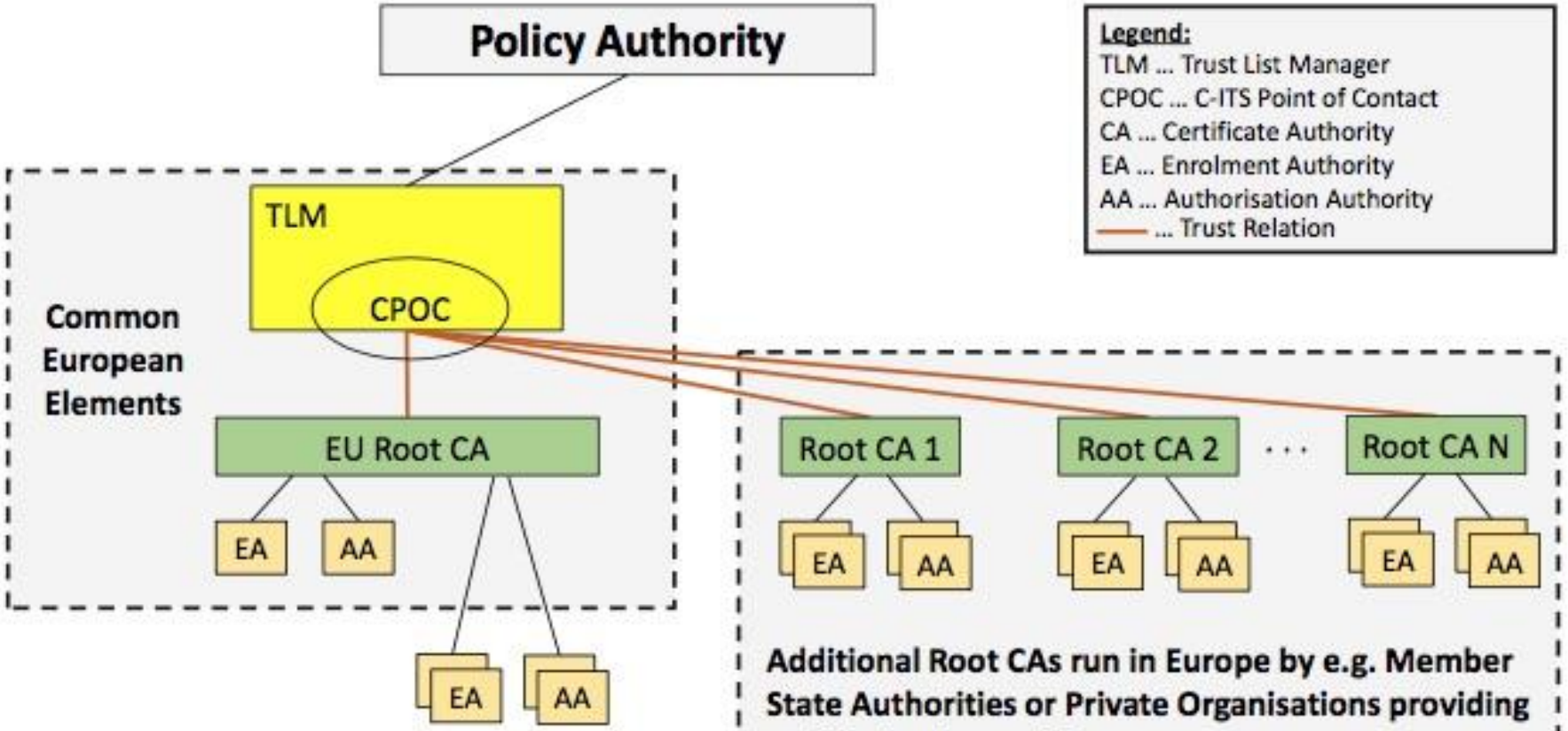


Figure 1: C-ITS Trust model architecture

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

セコムIS研究所
Intelligent Systems Laboratory

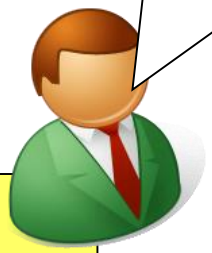
過去のPKI day の参考スライド

２０１１年現在の状況？

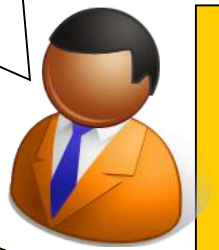
セコムIS研究所
Intelligent Systems Laboratory

"Rough consensus and running code"

法制度等から
ニュートラルな
技術標準



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。。」



ギャップ
噛み合わない会話
共有されないビジョン

技術標準

・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

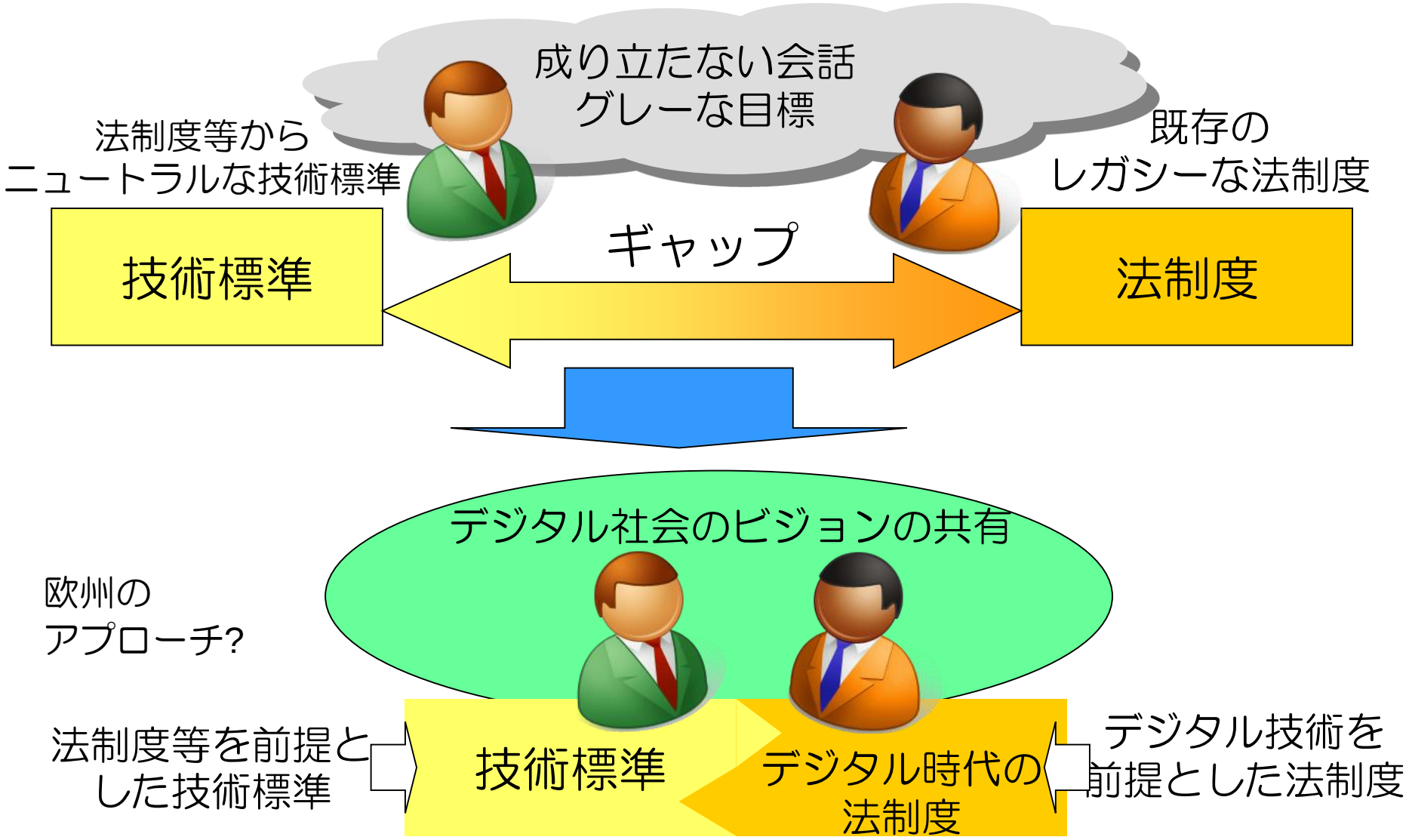
既存の慣習、権益が強すぎる問題

「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 2015のオーバビュー

セコムIS研究所
Intelligent Systems Laboratory

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

セコムIS研究所
Intelligent Systems Laboratory

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？

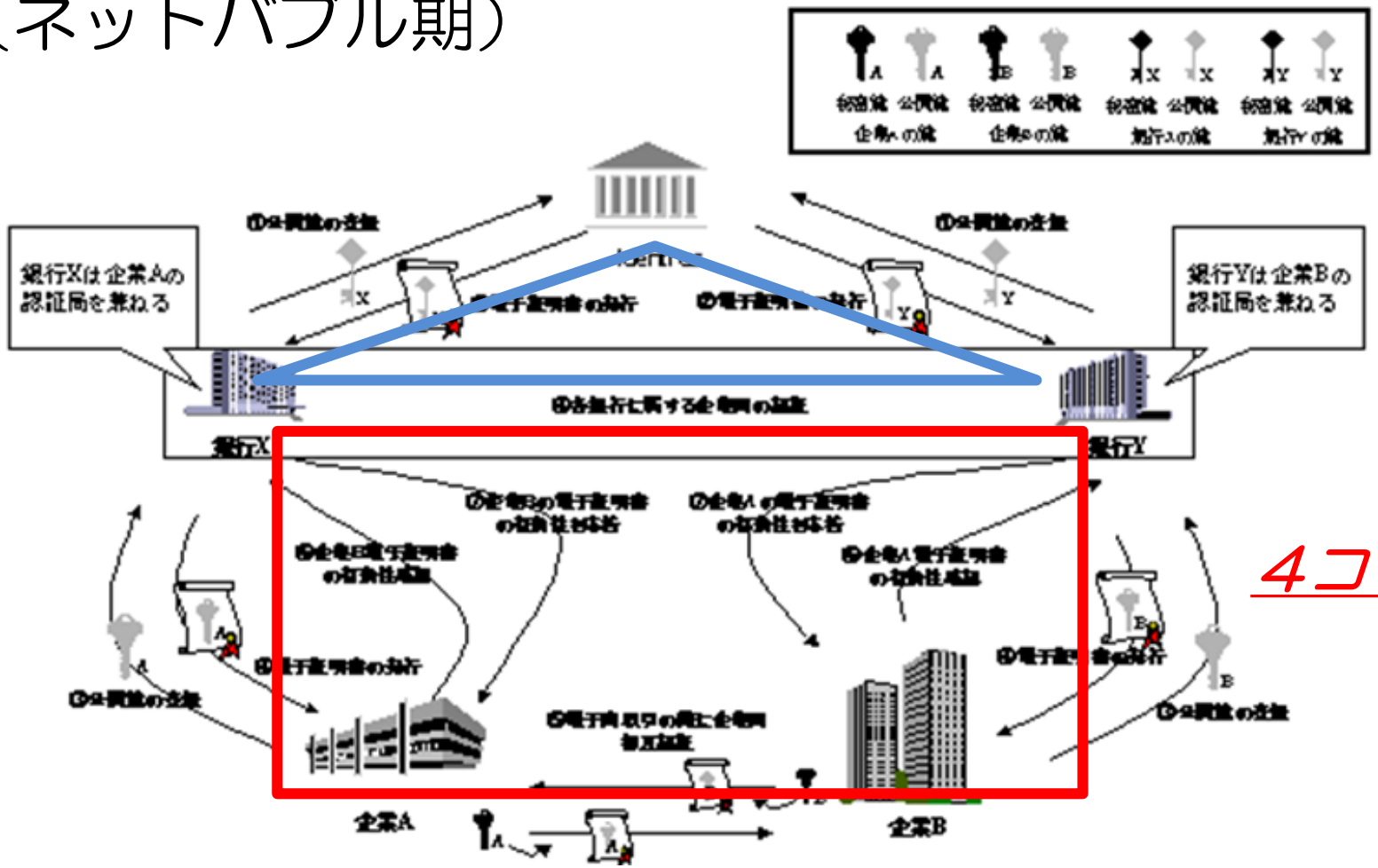
アイデンティティ管理（自然人、法人）
日本におけるマイナンバー制度等

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？

セコムIS研究所 Intelligent Systems Laboratory

- 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:I　dentrus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