

IoTに求められるトラストとJT2Aの活動

--超スマート社会（Society 5.0）におけるトラストの在り方--

2018年1月24日

松本 泰

JT2A副代表/

JNSA PKI相互運用技術WGリーダー/

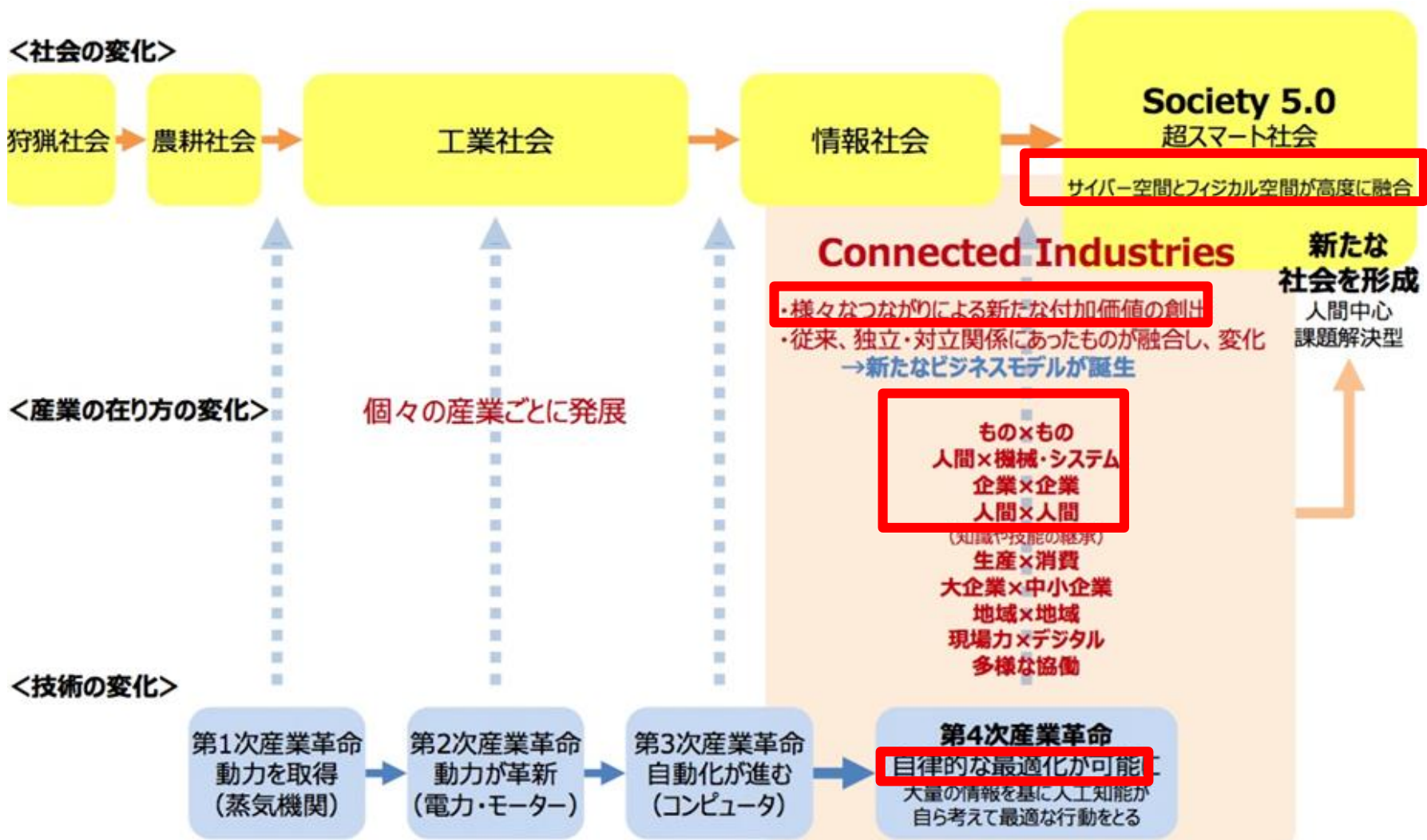
セコムIS研究所

- 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対応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だと言えます。
- 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、何らかの信頼と信頼関係が必要になり、この信頼が価値に結びつきます。
- 超スマート社会は、多様な人・モノ・サービス間の複雑な信頼関係が要求される社会とも言え、ここには、新たなトラストテクノロジーも求められています。
- こうした認識に基づき、今後の超スマート社会におけるトラストテクノロジーの役割と課題、そして、この課題解決をリードするJT2Aの期待をお話しします。

- (1) 超スマート社会・IoT・サイバーセキュリティ
- (2) IoTにおけるトラスト・テクノロジーの役割
- (3) Case study 車におけるトラスト・トテクノロジー
- (4) JT2Aの活動への期待

超スマート社会・IoT・サイバーセキュリティ

- ・ 超スマート社会におけるIoTの役割
- ・ 超スマート社会・IoTを下支えするサイバーセキュリティ
- ・ セキュリティ・プライバシー・トラスト



- ・ 「情報社会」から「超スマート社会」への移行に伴うセキュリティへの要求の変化
- ・ 「超スマート社会」におけるトラストの在り方

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



- 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させるIoTサービスシステム ≡ 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）
 - リア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
 - 判断結果等をリアル空間へ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

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 (トラスト・テクノロジー)

- 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 ⇒ 悪意ある第3者からの攻撃を防ぐ
- ・ 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
 - ・ 「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？

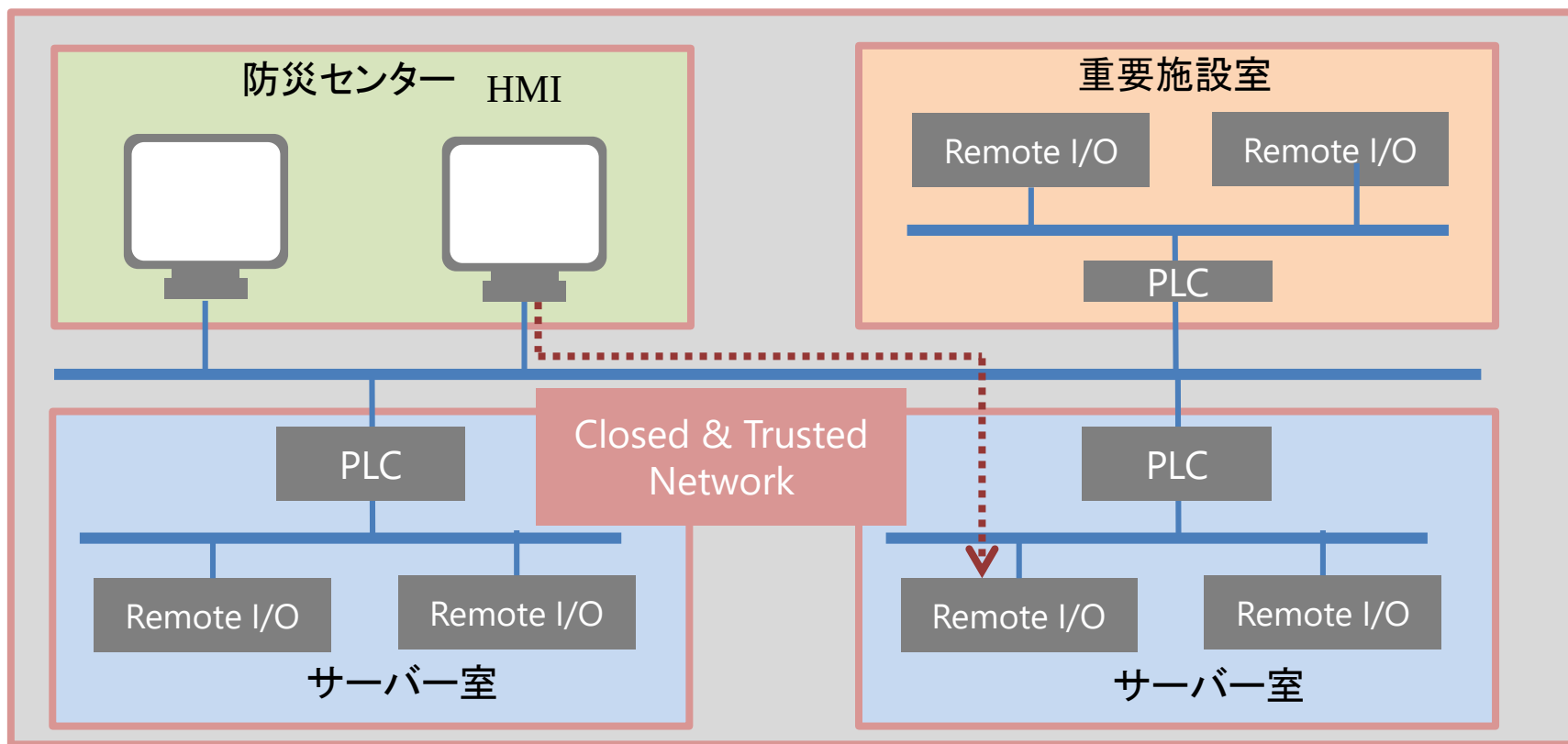
価値の創造のためには、Trust by designが必要でありトラストテクノロジーが重要な役割を果たす

IoTに求められるトラスト・テクノロジー

- ・ 「繋げることによる価値の創造」と価値の創造のための信頼、及び、信頼関係の構築
- ・ 超スマート社会において信頼関係を構築・社会実装するためのトラスト・テクノロジー

（現状の）重要インフラ・制御システムのセキュリティ JT2A

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

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



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

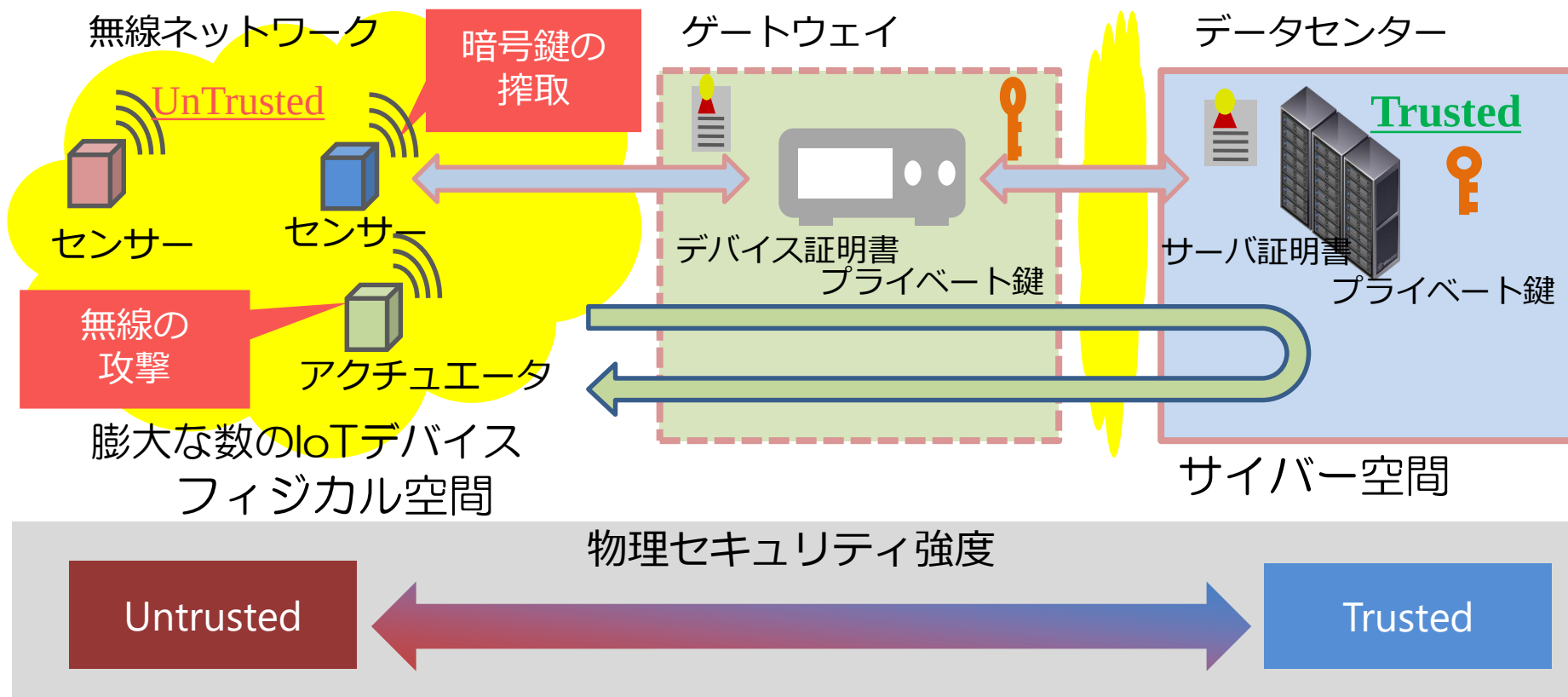


家 (弱い物理セキュリティ)

データセンター (強い物理セキュリティ)

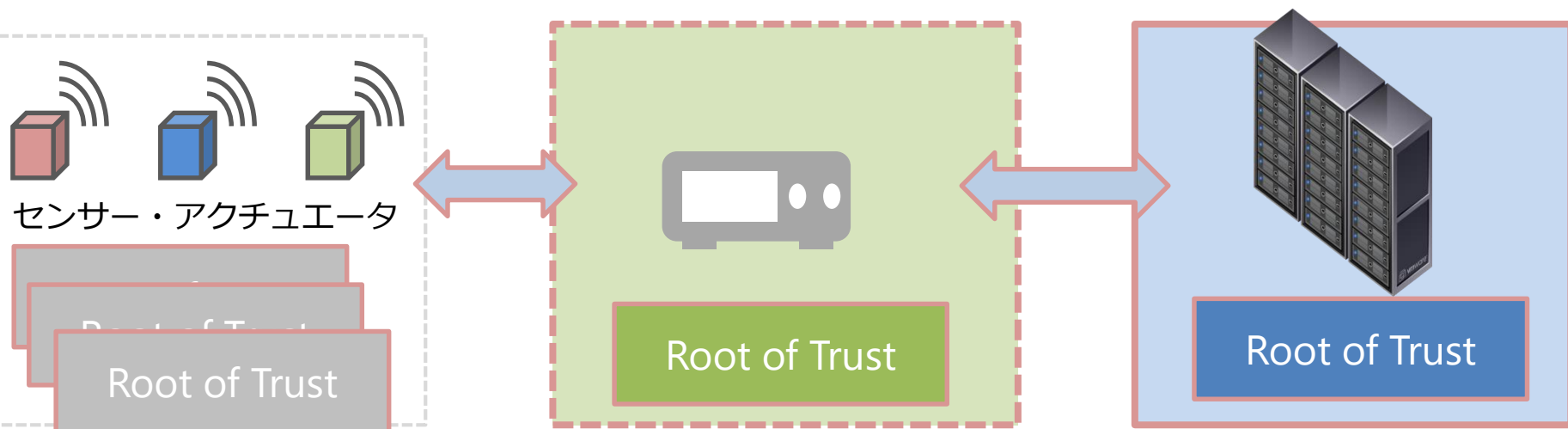
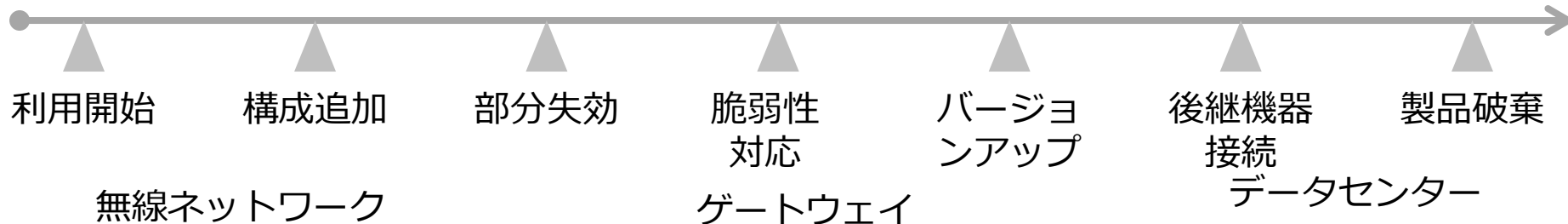
Untrustedなインターネットを介してTrustを確立するのがトラストテクノロジーの一つの目標だった。

「サイバー空間とフィジカル空間が高度に連携した社会」 CPS (Cyber Physical Systems) のためのトラスト



- 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、「**物理的環境に依存しないセキュリティ**」が求められる。
 - 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
 - 広く配置されるIoTデバイスを収容するための無線＋無線セキュリティ技術
- **必然的にフィジカル空間のIoTデバイスも含めた「トラストテクノロジー」が重要になる**

「サービス・イノベーション」のためのトラスト 長期のセキュアーな運用に耐えうるためのトラスト

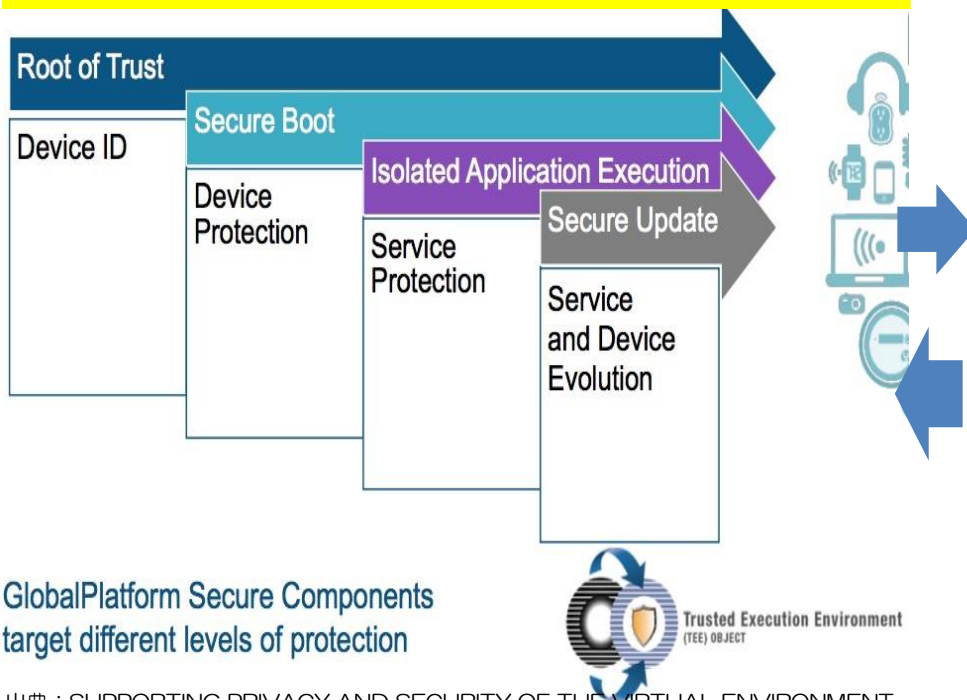


- IoTデバイスは、**長期の暗号鍵管理、クレデンシャル管理に耐えうるハードウェアセキュリティ**が重要
- IoTサービスシステムでは、**長期の信頼(=長期の暗号鍵管理、クレデンシャル管理)における運用**が重要

⇒ IoTに求められるトラストテクノロジー

個々のIoTデバイスの観点

Secure Hardware Root of Trust



GlobalPlatform Secure Components
target different levels of protection

出典：SUPPORTING PRIVACY AND SECURITY OF THE VIRTUAL ENVIRONMENT
https://docbox.etsi.org/Workshop/2017/201710_IoT/WORKSHOP/S06_SECURITYandPRIVACYinIoT/GLOBALPLATFORM_BERNABEU.pdf

CPS (Cyber Physical Systems) の観点

大量のIoTデバイス管理

アクセス制御・権限管理

クレデンシャル管理

暗号鍵管理

ビッグデータ管理(ライフサイクル管理)

署名された
ビッグデータ

暗号化された
ビッグデータ

暗号鍵（署名鍵、暗号化鍵）管理

サービスの視点から見たIoTビジネス及びIoTセキュリティにおいて重要なのは、多様なステークホルダー、エンティティとの信頼関係を維持するために、**大量**のIoTデバイスを、**長期**に渡り**セキュア**で**効率的**な管理が、適切なコストで出来ることになる。

Case study

車におけるトラストテクノロジーの動向

-- 第4次産業革命に対応した車のためのトラストテクノロジー --

- 第4次産業革命に対応した 車のCASE化とCASE化を支えるトラスト
 - 車と外部のサービス間のトラスト
 - ✓ 安全・安心・便利・快適等を提供するサービスイノベーションのためのトラスト
 - ✓ OTAの様な場所依存から場所に依存しないリモート保守
 - ✓ コネクテッドカー、スマートカー、クラウドサービスとの連携
 - 車内のECU等の間のトラスト
 - ✓ 製造のサプライチェーン&サプライチェーン・インテグリティ)
 - ✓ 自動運転等に向けて、ECU間の高度な連携が求められる
 - ✓ ex. ECUに格納されたダイナミックマップを参照しながら自動走行

JT2A

- 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。



(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???

CASE化を支えるCybersecurity

誰がコスト負担???

Security

Privacy

Trust

Safety

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高い。
Privacy, Trustは、ビジネスデザインでもある

誰がコスト負担 ⇒ サービスイノベーションがコストを吸収????

- 現在進行中、検討中の車におけるトラスト・テクノロジー
 - 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)
- CASEの観点
 - 「Connected (コネクテッド)」
 - 「Autonomous (自動運転)」
 - 「Shared & Services (共有化&サービス)」
 - 「Electric (電動化)」

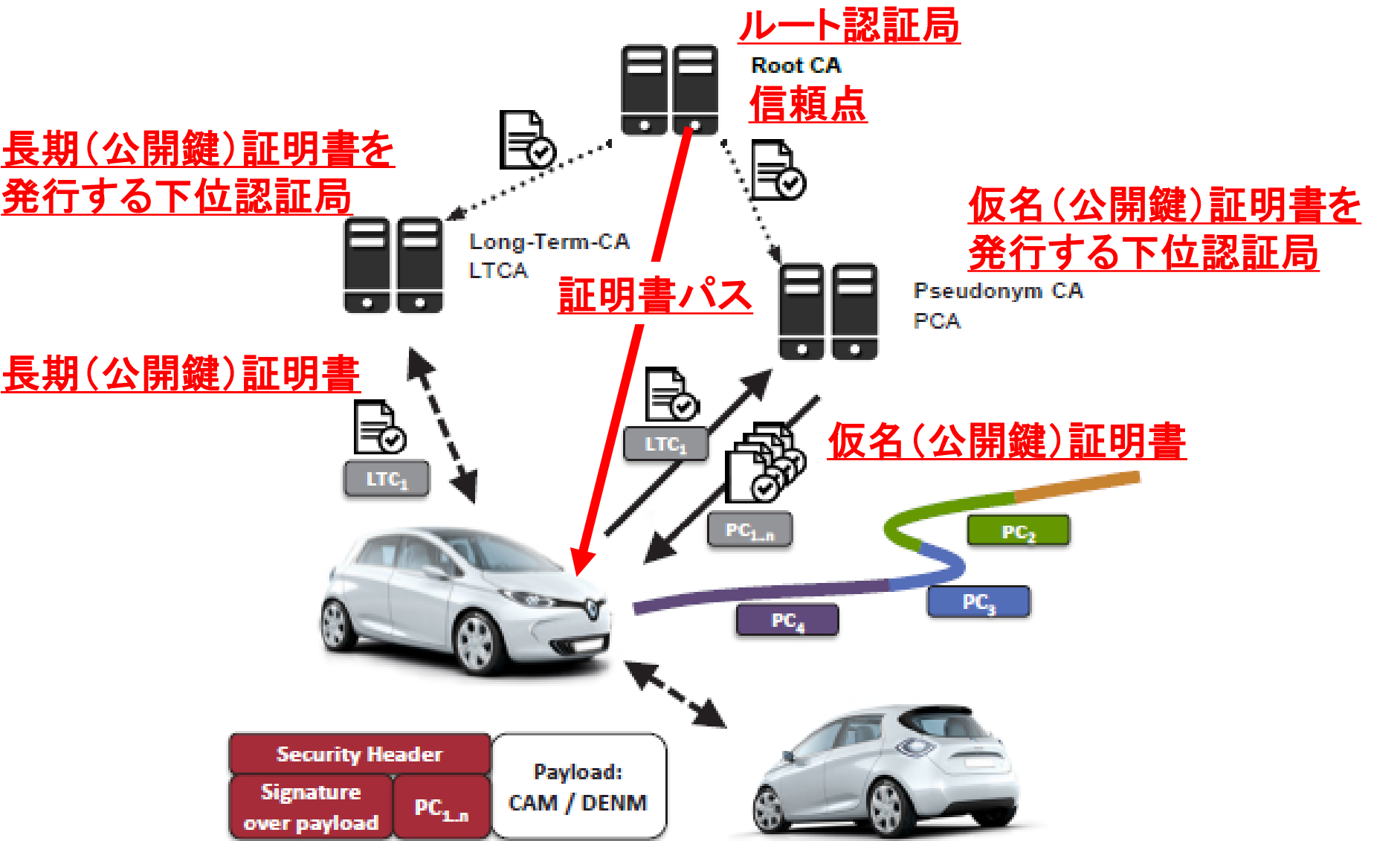
欧州のR&Dプロジェクトの比較

	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

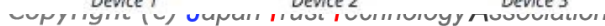
- Evita Prj.の成果のIntra-vehicle security が、SHE（Secure Hardware Extension）として、ECUに組み込まれつつある。
- Preserve Prj.の成果であるInter-vehicle security として、欧州のITS-C等の実証実験を経てPKI（公開鍵基盤）の構築と車への組み込み等が本格する??

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



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

JT2A



<https://www.its.dot.gov/pilots/index.htm>

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

<https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/connected-vehicle-security.pdf>

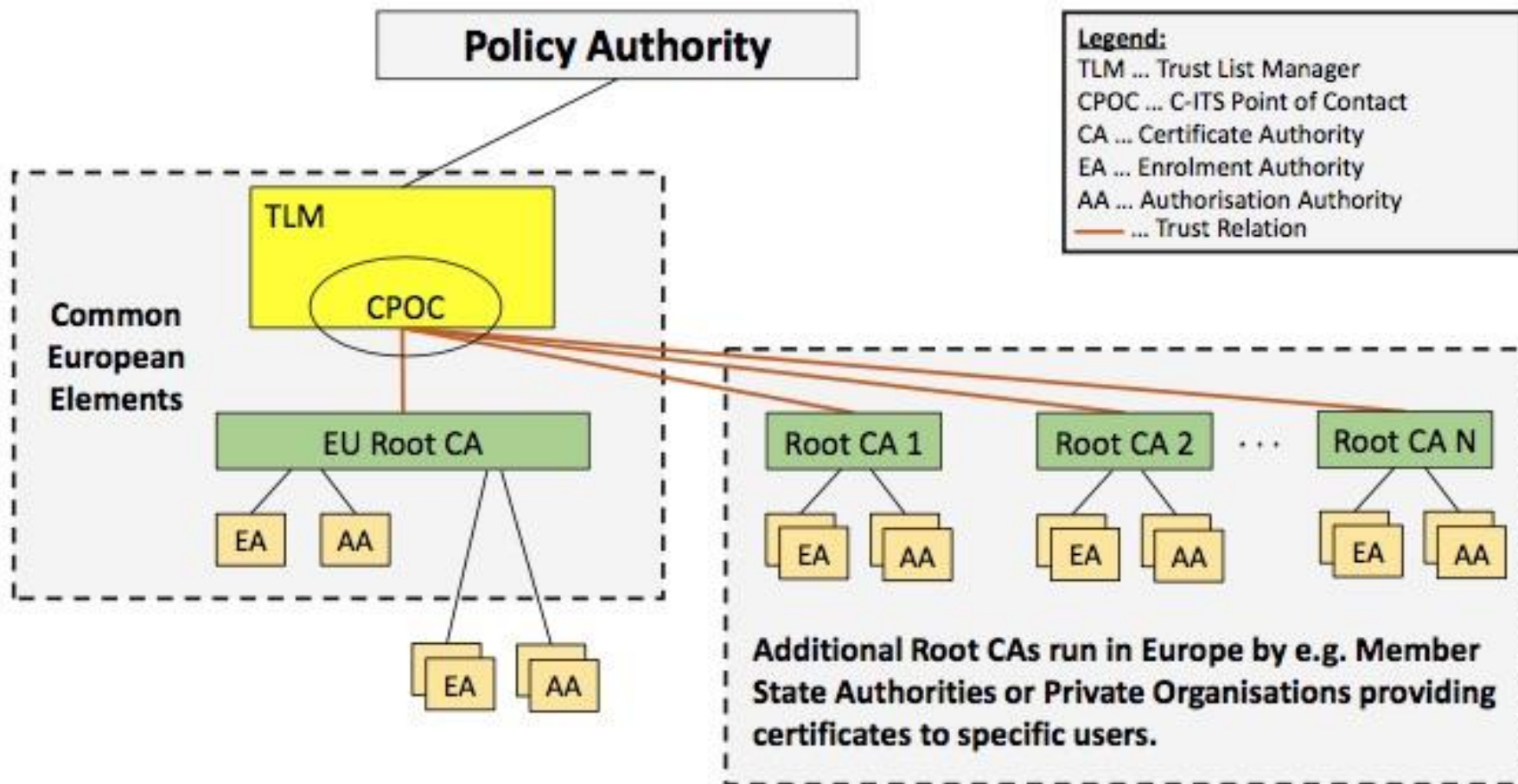


Figure 1: C-ITS Trust model architecture

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

JT2Aの活動への期待

- 「超スマート社会」は、効率的で、透明性があり競争力のある社会であるべき
- そのためには、トラスト・テクノロジーが重要な役割を担う必要がある



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..



- 2001年に施行された電子署名法は、人（自然人）が作成した紙の書面への署名や捺印と同等の効力を、デジタル文書に与えようとしたものでしたが、こうしたことの重要性は、「情報社会」における必然であり、これは現在でも変わりません。
- しかし、既存の紙文書を前提とした業務プロセス等をデジタル文書に置き換えるだけでは、人の作業がボトルネックになり、大きな効率化は望めないことも認識されてきました。
- 「情報社会」の次の「超スマート社会」は、業務プロセス自体を変革し、人の関与を最小限した自律的に機能するデジタル・トランスフォーメーションを目指した社会かもしれませんが、ここにこそ、電子署名等が大きな役割を果たすべきです。
- 更に「サイバー空間とフィジカル空間が高度に融合した社会」においては、電子署名法における人（自然人）以外に、多様な人・モノ・サービス間の大量の信頼関係が必要になることも必然であり、この繋がる社会にこそ、トラスト・テクノロジーが、より重要な役割を果たす必要があるとも言えます。
- また、第4次産業革命、この革命に対応する社会への移行には、多くの法制度的な課題もあります。
- JT2Aの活動では、超スマート社会に必要とされるトラスト・テクノロジーを追及するとともに、「革命」に必要な法制度のあり方の提言、そして、デジタル・トランスフォーメーションやサービスイノベーションなどのビジネスの確立を目指した活動を期待しています。

参考スライド

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??

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

プログラム
(コード署名)

電子領収書

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