信頼される安心を、社会へ。
SECOM

データ戦略のためのITシステム
--IoTとはデータ戦略である--

2019年11月27日

松本　泰　セコム（株）ＩＳ研究所

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
- 2019年11月現在
  - CRYPTREC　量子コンピュータ時代に向けた暗号の在り方検討TF　委員
  - 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　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）
  - JEITA スマートホーム部会　スマートホームセキュリティWG 主査

データ戦略の課題と未来
データ戦略のためのＩＴシステム　-- IoTとはデータ戦略である

- 「データ戦略の課題と未来」⇒「データ戦略の（ほんの少し）未来の課題」
- 「データ戦略のためのＩＴシステム」これを少し拡大解釈して、Soceity5.0時代のITシステムは、IoTを駆使したサイバー・フィジカル・システム
- 「IoTとはデータ戦略である」
  - データ戦略のベースとなるデータソースは、IoTデバイス・エッジAI
  - エッジAIが出力するデータソース⇒ 機械学習⇒学習済モデル⇒エッジAI⇒エッジAIの実行結果等⇒サイバー空間へ　-- この循環を作り上げるのがデータ戦略
- そもそも何のためのデータ戦略なのか??
  - 「フィジカル空間におけるサービスイノベーション」のためのIoT&データ戦略
    - ⇒ 「IoTとはデータ戦略である」の意味するところ
- 「データ戦略の課題と未来」　≒　Soceity5.0時代データ戦略
  - サイバー・フィジカル・システムにおけるビジネスデザイン、法制度・法務コンプライアンス、技術アーキテクチャを俯瞰した上でのデータ戦略が重要
  - そうした中、トラストの観点が重要になっていく → デジタル社会におけるトラスト

IoT ・BD・AI ≒ サイバーフィジカルシステム

サービスイノベーションのための新たなデジタルプラットフォーム

信頼される安心を、社会へ。 SECOM

法と技術アーキテクチャ

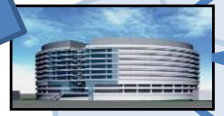
技術

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

ITシステムからサイバーフィジカルシステムへの発想転換
データ戦略のベースとなるデータソースのパラダイムシフト

- 2000年台
  - PC等で、（プロフェッショナルな）人が入力するデータ
- 2010年台　　現在のデータ戦略におけるデータソース
  - （汎用的な）モバイルデバイス・スマートフォンで、人が入力するデータ＋α（位置情報等）が、クラウドへ集約
    - →　たぶん、本日の話題の中心は、この辺り？？
- 2020年台　　これからのデータ戦略におけるデータソース
  - 空気のように遍在するIoTデバイスが吐き出すデータ
    - →　松本の話は、このあたり？？

- サイバー・フィジカル・システムにおける価値あるデータ、信頼のおけるデータとは。その際必要となるIoTデバイスとは。

フィジカル空間におけるサービスイノベーションのためのデータ戦略
これらを支えるセキュリティ・プライバシー・トラスト

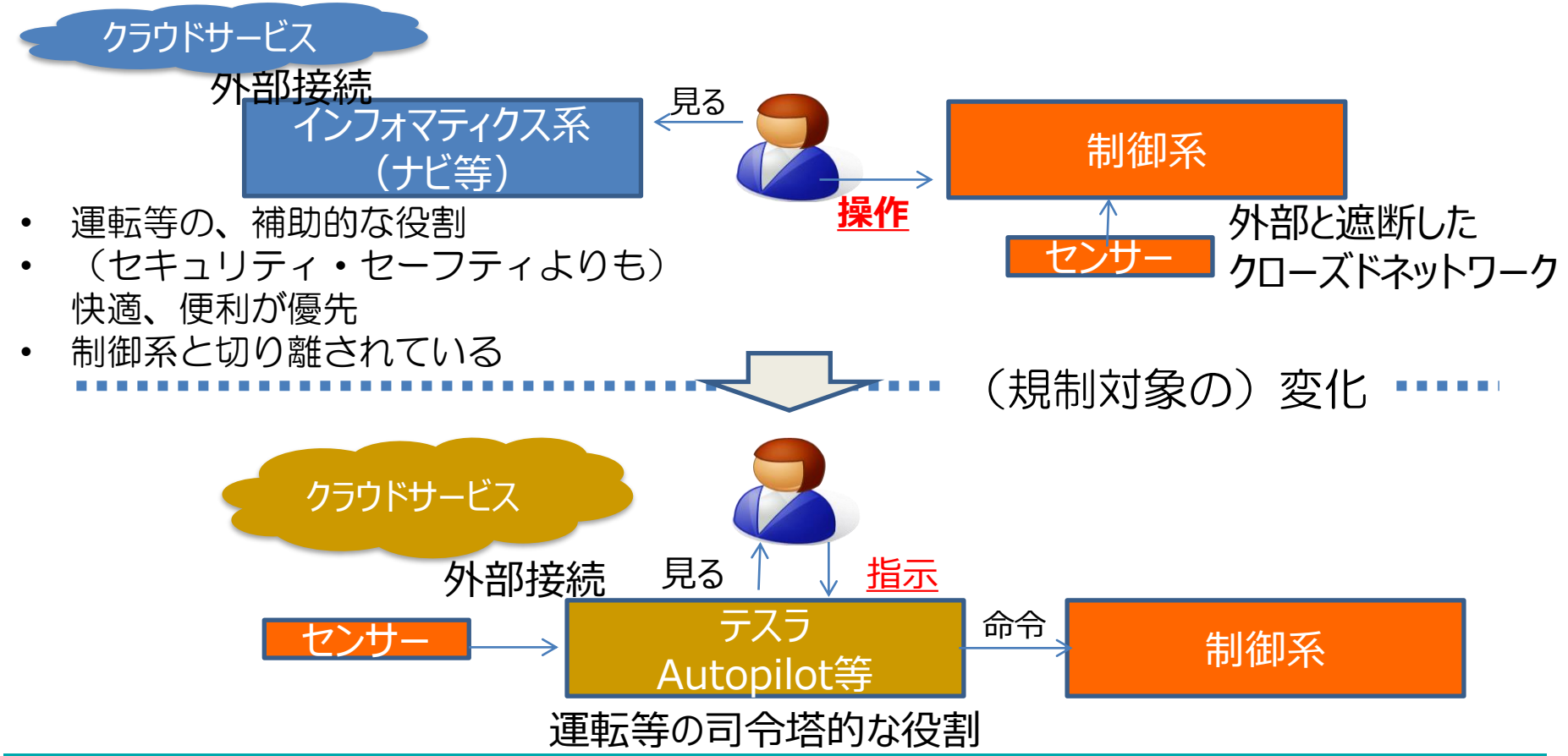
- セキュリティ　　IoTセキュリティ、サイバー・フィジカル・セキュリティ
  - 主に悪意ある第３者からの攻撃の対策　-- 様々な議論が進行中
- プライバシー　　価値あるデータはパーソナルデータ、IoT的課題も多々ある
  - ビジネス　　個人情報の保護と利活用のバランスないし両立
  - 法制度　　改正個人情報保護法、GDPR対応とか
  - 技術アーキテクチャ　C.I.A.のConfidentiality, AvailabilityをIを両立する実装技術
- トラスト　　Soceity5.0時代のトラスト
  - ビジネス　　顧客を含むステークホルダー間の信頼関係の構築
    - サブスクリプション・ビジネスモデルにとって非常に重要
  - 法制度　　トランスペアレンシー、トレーサビリティ、アカウンタビイティ
  - 技術アーキテクチャ　C.I.A.のIntegrity ⇒　インテグリティの実装技術
    - 膨大な数のIoTデバイス・AIエッジとデータ。このインテグリティ

トラスト・法制度からの要求　--　規制のパラダイムシフト
エッジAI（自動車、医療デバイス）の場合　--　IoTの方向性のひとつ

信頼される安心を、社会へ。
SECOM

- 実現したいこと、されようとしていること　--　自動運転、AI診療など
  - ハードウェア（だけ）からソフトウェアへ、AI・学習済モデル等の利用
  - 大量のIoTデバイスをフィジカル空間に配置し、大量のデータをサイバー空間に吸い上げ、そして学習（AI）し学習済モデルを生成、学習済モデルをIoTデバイス（エッジAI）へ
    - → デジタル・ツイン、データの循環
  - OTA(Over The Air)による製品出荷後の改良、新機能の追加、リモート管理。
  - リモート管理による運用／保守等コスト削減、etc.　⇒膨大な数のIoTデバイス
    - ⇒　リモート管理による「フィジカル空間おけるサービスイノベーション」へ
- 規制のパラダイムシフト　　→　　参考スライド　18, 19
  - 製品（単体）の規制（型式認証、出荷時検査）からサービスシステムの規制へ
    - 製品出荷後の、トレーサビリティ・トラッキングの要求
  - エッジAI等ブラックボックス化するサービス・システムに対するトランスペアレンシー
  - インシデント等に対するアカウンタビリティ、リーガルリスク対応
    - インシデント → セーフティー（侵害）、プライバシー侵害、セキュリティ脆弱性

トラスト・法制度からの要求　--　規制のパラダイムシフト
車のアーキテクチャが変る->外部接続の意味が変る->データ戦略も変る



- 運転等の、補助的な役割
- （セキュリティ・セーフティよりも）
  快適、便利が優先
- 制御系と切り離されている

トラスト・法制度からの要求　－　インテグリティの実装
CASE化に向かう自動車の場合

- 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（自動車のVIN等）とソフトウェアー更新、学習済モデル更新の証跡管理など
- アカウンタビリティ(accountability)
  - インシデント時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の対応

- 法制度の対応と、実現するための技術への要求
  - 膨大な数のIoTデバイス、高機能化するエッジAIを利用するサイバーフィジカルシステムにおける「トレーサビリティ・アカウンタビリティ・トランスペアレンシー」への要求を効率的に対応するための実装
- ⇒　トラストなIoTデバイスと暗号技術を駆使したシステム全体のインテグリティ

トラスト・技術（IoTデバイスのイノベーション）

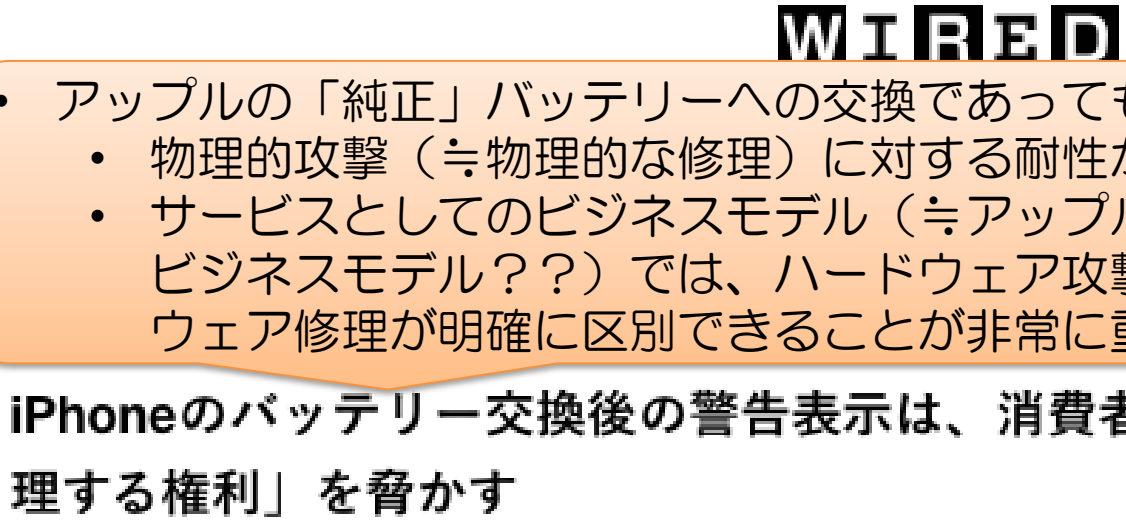
信頼される安心を、社会へ。
SECOM

- IoTのイノベーションを理解する鍵　　IPとSoC
  - #Internet Protocol とSecurity Operation Center ではない
  - IoTデバイスの実体は、大量産可能なSoC （System-on-a-Chip）
  - SoCのコストは、限りなくシリコンコストへ--巨大なファブは、巨大な印刷工場
  - SoCの設計パーツであるIPコア（Intellectual Property core）のオープンソース化
    - 高機能なIoTデバイス（エッジAI等）も低コスト化
  - →　サイバー・フィジカル・システムの課題は、IoTデバイスの製造コストではなく、IoTデバイスの管理・運用コストへ
- トラストなIoTデバイス　→　　ここにも、大きな進展がある　→　参考スライド　20、21
  - ハードウェアセキュリティを具備したSoC（System-on-a-Chip）
    - #物理的な運用＆セキュリティのコストを大幅に削減できる可能性
  - 信頼のおけるデータを吐き出すIoTデバイス
    - 高度な暗号技術が組み込まれた（安価な）IoTデバイス
  - IoTデバイスをリモート管理可能な標準化　　→　参考スライド　22
    - IETFにおけるIoTセキュリティ標準化等

修理する権利の話
right-to-repair
NEWS

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/

- 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


WIRED

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
テリーに問題が
一側はセキュリ
張しているが、
脅かす可能性がある。

- 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*

トラスト・IoTの技術　－　インテグリティの実装技術
法制度的にも理解されるべきテクニカルターム

- Root Of Trust　--　最も重要なテクニカルターム・暗号技術的な用語
  - IoTデバイスに格納された暗号鍵によるトラストアンカー＆デジタル署名によるトラストチェーン（ないしChain Of Trust)の検証 -> 暗号技術・デジタル署名によるインテグリティの検証、目視に頼らないインテグリティの検証
- ハードウェアセキュリティ
  - フィジカル空間に（空気のように）散在するIoTデバイスの物理的攻撃の対応
  - ハードウェアによるトラストアンカー& Root Of Trustとなる暗号鍵の保護
  - HW Root Of Trust , シリコンRoot Of Trust　-> 参考スライド 20
- TEE　（Trusted Execution Environment）
  - 例えばアプリケーションを監査するLegal VM (Virtual Machines)の実装
- リモートアテステーション（ Remote ATtestation ）
  - TEEなどを利用したリモートからのアプリケーション・デバイス構成管理
  - サイバーフィジカルシステムにおけるデジタル監査へ

インテグリティ実装のパラダイムシフト
→ Auditing & Attestation パラダイムシフト

信頼される安心を、社会へ。
SECOM

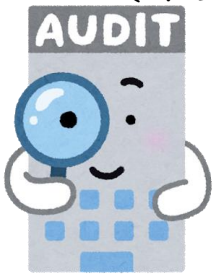
データソース

曖昧さ、間違い、改ざんの可能性を内包したデータ

データクレンジング等の作業

データベース

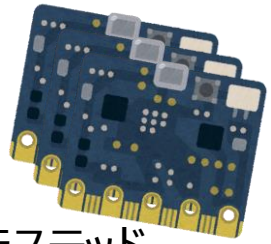
目視による整合性チェック（インテグリティチェック）



Auditing & Attestation
監査及び証明業務（アテステーション）

一意なデバイスIDと、リモートアテステーションにより管理されたIoTデバイスを前提に設計されたデータベース

データソース

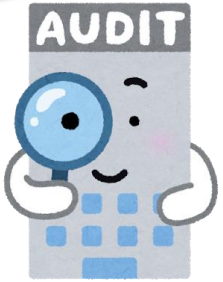


トラステッド IoTデバイス

デジタル署名付きデータ

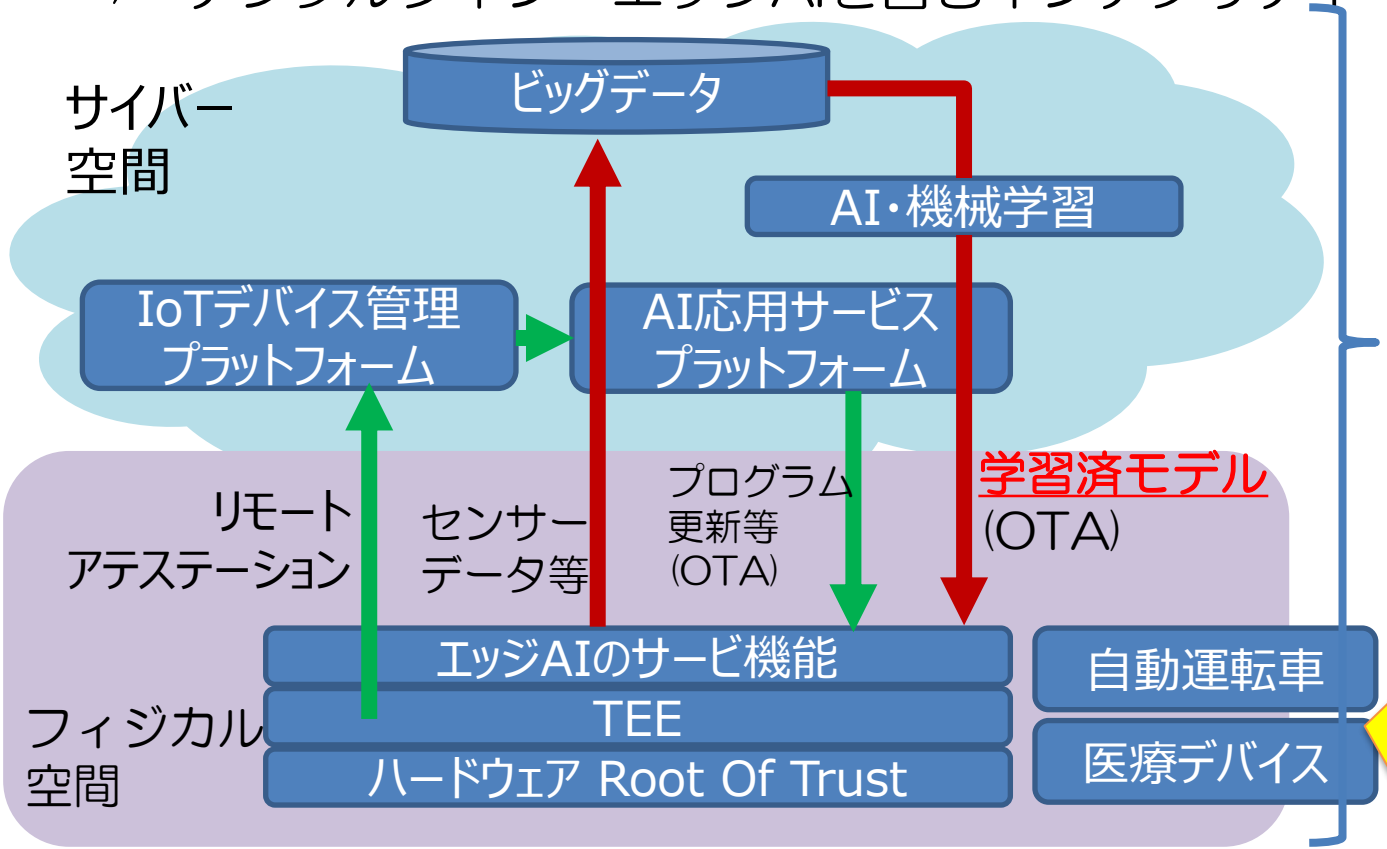
リモート アテステーション（構成管理）

クラウドサービス データベース



自動化されたデジタル署名の検証、トラストチェーンの検証によるインテグリティチェック

トラスト・技術アーキテクチャ
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



- この循環がデータ戦略であり、この「系」全体のインテグリティが必要
- 膨大な数のIoTデバイス
- 高機能なエッジAI

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

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

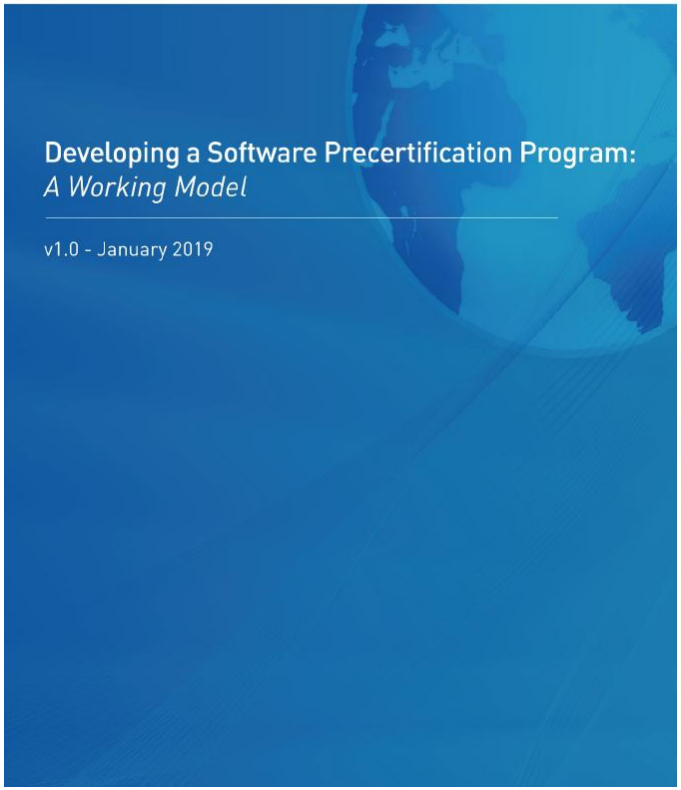
IoTデバイスからすると管理者不在で信頼できない環境（物理的、ネットワーク的）

おわりに「データ戦略の課題と未来」≒Soceity5.0時代データ戦略

- これからの時代（Society5.0・IoT・AI・BD時代）のデータ戦略では、「トラスト」が重要なキーワードになる。
- ビジネスデザインとトラスト
  - サブスクリプション・ビジネスモデル等における顧客とサービス間、IoTデバイスと顧客間のビジネス上のトラスト
- 法制度、法務コンプライアンスとトラスト
  - 膨大な数のIoTデバイス、高機能なエッジAIから構成されるサイバーフィジカルシステムに対する法的規制、リーガルリスクに対応するためのトラスト
- 技術アーキテクチャとトラスト
  - ビジネス、法制度の要求を効率的に実現するための暗号技術とハードウェアセキュリティ等により実現されるIoTデバイスとデータのトラスト
- ビジネスデザイン、法制度、技術アーキテクチャ、それぞれのトラストが考慮されたデータ戦略が、新たな時代のデジタルプラットフォームを作ると考えられる。

参考スライド

規制のパラダイムシフト
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



- “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。

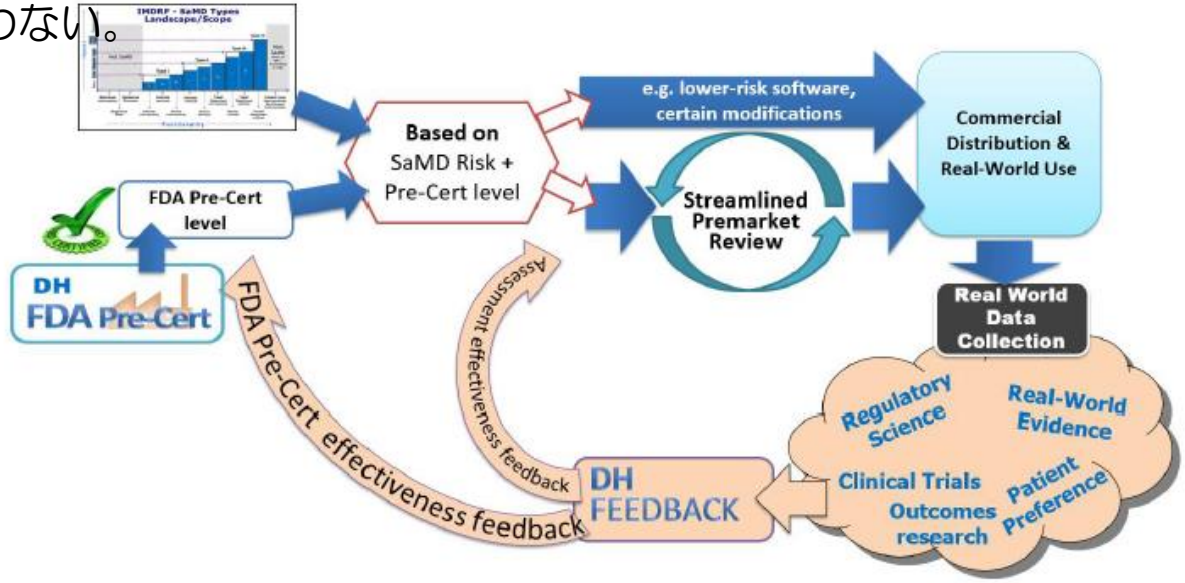
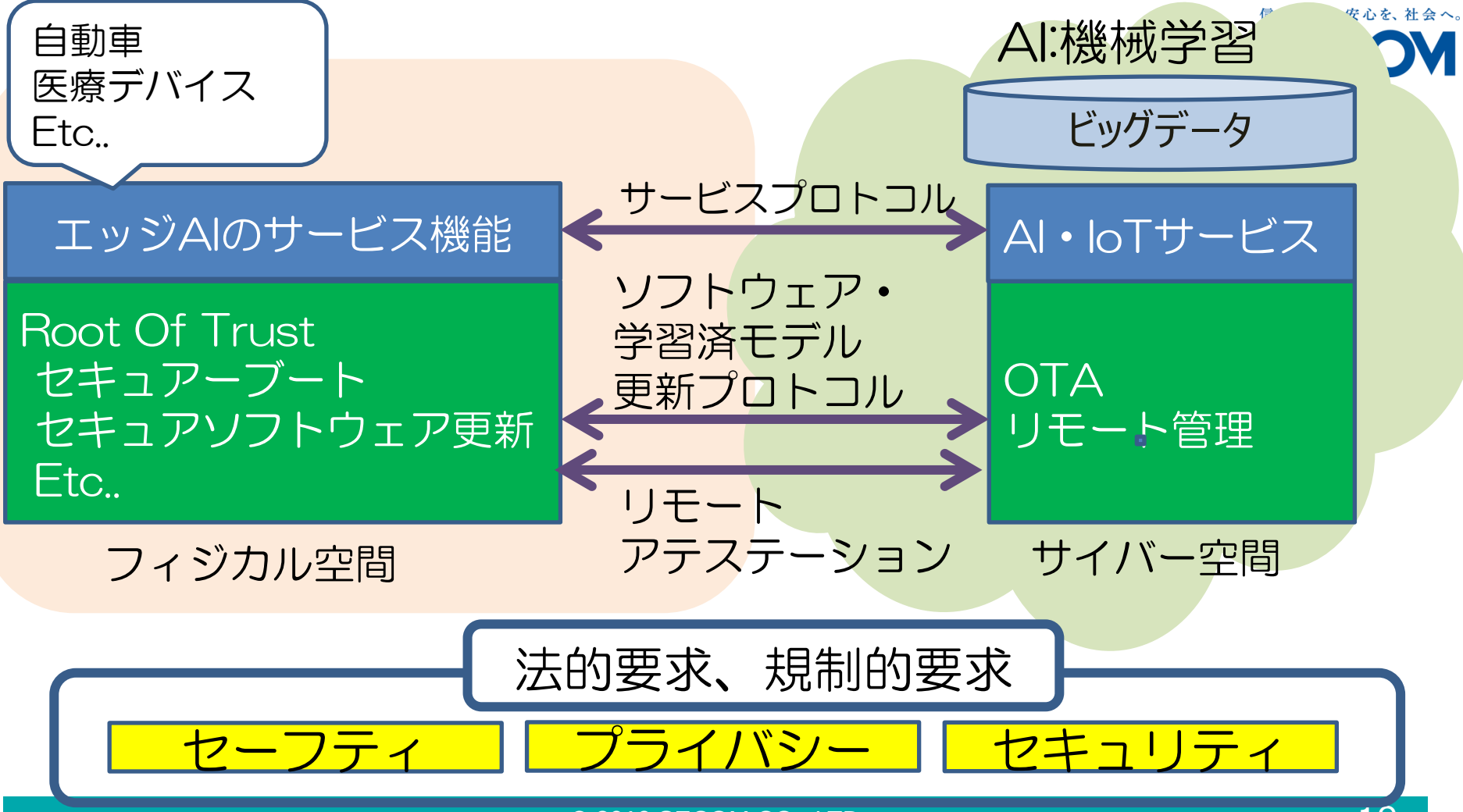


Figure 1. A reimagined approach for the regulation of software

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



OpenTitan – 透明性、安全性、信頼性の高いシリコン チップ設計をオープンソース化　2019年11月6日

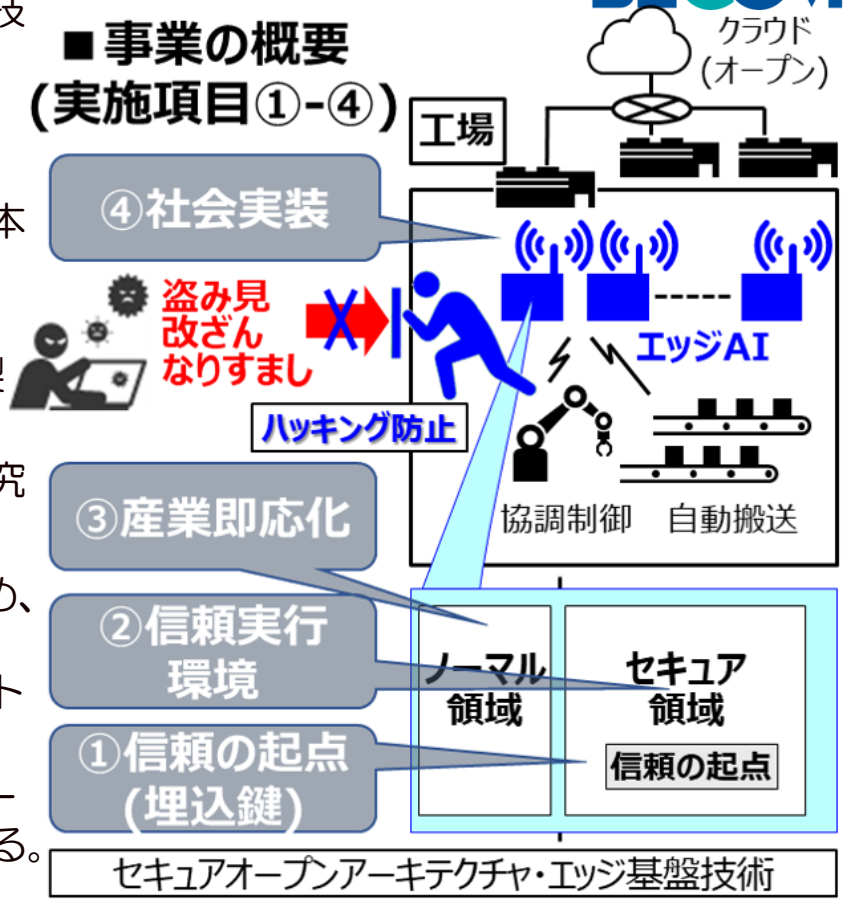
- セキュリティは安全なインフラストラクチャから始まります。インフラストラクチャのセキュリティと完全性への信頼を高めるには、特別な専用チップを使用して、基盤の部分の信頼性を確固たるものにする必要があります。
- 本日 Google は、パートナー各社とともに、シリコン レベルの RoT（Root of Trust：信頼の基点）プロジェクトとしては初めてのオープンソースとなる OpenTitan を発表しました。OpenTitan は、データセンターのサーバー、ストレージ、周辺機器などに合わせた高品質なデザインを提供します。シリコン設計をオープンソース化することで、従来よりも分かりやすく信頼性も高まり、最終的には安全性が向上します。
- シリコンで信頼を支える
  - シリコン RoT は、承認された検証可能なコードを使用し基幹システムのコンポーネントが安全に起動することを確認することで、ハードウェア インフラストラクチャとその上で実行されるソフトウェアが信頼性の高い状態を保つために役立ちます。シリコン RoT は以下を支援することにより多くのセキュリティー上のメリットを提供します。（中略）
- 透明性とセキュリティ基準の引き上げ
  - （以後、省略）

出典： https://cloud.google.com/blog/ja/products/identity-security/opentitan-open-sourcing-transparent

セキュアオープンアーキテクチャ・エッジ基盤技術研究組

- 名称：セキュアオープンアーキテクチャ・エッジ基盤技術研究組合
- 設立年月日：2019年8月28日設立
- 理事長：鮫嶋　茂稔（(株) 日立製作所　研究開発グループ　テクノロジーイノベーション統括本部　統括本部長）
- 組合員：（株）エヌエスアイテクス、（学）慶應義塾、(国研) 産業技術総合研究所、セコム (株)、（株）日立製作所、【３企業１国研１学校】
- 事業の概要：AIエッジ向けセキュリティ技術の試験研究
- ○組合設立の目的:
- (1) 半導体チップのセキュリティを検証可能とするため、RISC-Vオープンアーキテクチャを活用し、セキュリティのハードウェア・ソフトウェア基盤技術をホワイトボックス化する試験研究を実施する。
- (2) セキュリティ技術の協調領域として開発技術をオープン化し、AIエッジデバイスの実用化、普及を促進する。

出典：http://trasio.org/home/



なぜIETF--「クラウドとハードウェアのエコシステム」交流の場 IoTデバイスをリモート管理するためのプロトコルの標準化

信頼される安心を、社会へ。 SECOM

- 制約デバイス -- IETFにおけるIoTデバイスのコンセンサス
  - RFC 7228 Terminology for Constrained-Node Networks
- SUIT-- IoTデバイスのソフトウェア更新
  - Software Updates for Internet of Things
- TEEP --TEE、信頼できる実行環境へのプロビジョニング
  - Trusted Execution Environment Provisioning
- RATs -- IoTデバイスのリモート健全性検証
  - Remote ATtestation ProcedureS
- MUD　RFC 8520
  - Manufacturer Usage Description Specification
  - IoTデバイスの通信ポリシーの標準フォーマット化