



モノの本物性を確認するために

2019/4/15

一般社団法人セキュアIoTプラットフォーム協議会

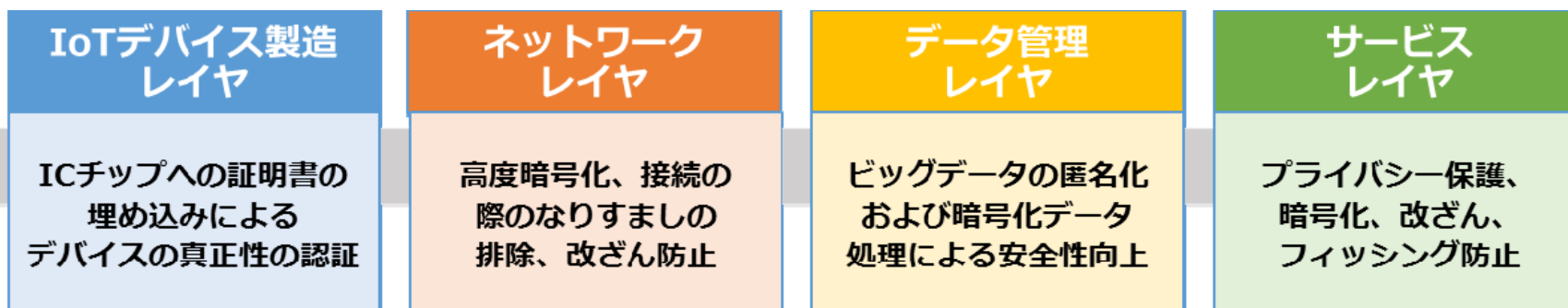
主席研究員

松本義和

一社)セキュアIoTプラットフォーム協議会 設立趣旨

セキュアIoTプラットフォーム協議会は、日本の産業界の知見を集約し、全世界のIoT機器およびサービスに対し、安心・安全な新社会基盤を創出する。

安心・安全にIoT機器やそのサービスを活用できるよう、
政府方針/ガイドラインの具現化に向け、
民間の力をあわせたオープンイノベーションにより、
IoT機器の製造段階から、クラウド環境でのサービスまで包含した
セキュリティ基盤構築の取り組みを推進する。



協議会概要



事業	・次世代IoTセキュリティ標準の規格化およびデファクトスタンダード化に向けての普及活動 ・IoT利活用推進および事例構築 ・共同実証実験(POC)の実施 ・最新IoT関連情報の発信 ・セキュリティ人材の育成
設立年月日	2017年4月3日
法人形態	一般社団法人
参加企業種別	【正会員】 ・半導体メーカー ・クラウドサービス事業者 ・データアナリティクスサービス事業者 ・アプリケーション開発ベンダー ・サービス提供事業者 ・IoT機器製造メーカー ・データセンター事業者 ・セキュリティベンダー ・システムインテグレーター 【賛助会員】 ・関連協議会 ・自治体 ・大学/学術機関
役員構成	・理事長：辻井重男（中央大学研究開発機構フェロー・機構教授、東京工業大学名誉教授） ・理事：佐野勝大（株式会社ユビキタスAIコーポレーション 取締役） 白鳥則郎（中央大学研究開発機構 教授） 田口勉（株式会社アイネット 上席顧問） 藤川春久（セコムトラストシステムズ株式会社 取締役） 眞柄泰利（サイバートラスト株式会社 代表取締役社長） 三木俊明（株式会社ラック 取締役 常務執行役員） ・監事：佐々木良一（東京電機大学総合研究所特命教授兼サイバーセキュリティ研究所所長） 宗像義恵（ビーグローブ株式会社 代表取締役、元インテル 副社長）、 森本登志男（前佐賀県最高情報統括監(CIO)、総務省地域情報化アドバイザー）
会費	・入会金：10万円 ・正会員：年会費20万円、賛助会員：無料 ・初年度会費は、入会時期によって2期に分けて設定（4～9月入会:20万円/10～3月入会:10万円）
HP	https://www.secureiotplatform.org/

参加企業(2019年3月31日現在)

【正会員：46社】

- Arm Ltd.
- IARシステムズ株式会社
- アイティーエム株式会社
- 株式会社アイネット
- 株式会社網屋
- 株式会社イメージア・ソリューション
- インタープラン株式会社
- 株式会社うぶすな
- エナジー・ソリューションズ株式会社
- 株式会社エヌ・ティ・ティ・データ
- F5ネットワークスジャパン合同会社
- 株式会社オービックビジネスコンサルタント
- クオリティソフト株式会社
- サイバートラスト株式会社
- 株式会社サイファースセキュリティ
- JIG-SAW株式会社
- 株式会社シーイーシー
- ジャパンインテグレーション株式会社
- 株式会社SYNCRHRO
- セコムトラストシステムズ株式会社
- ソフトバンク・テクノロジー株式会社
- 株式会社ソリトンシステムズ
- 大日本印刷株式会社
- 株式会社DTSインサイト
- 株式会社テリロジー
- 東京海上日動火災保険株式会社
- 東芝情報システム株式会社
- 東芝デベロップメントエンジニアリング株式会社
- 株式会社東陽テクニカ
- 凸版印刷株式会社
- トッパン・フォームズ株式会社
- トライポッドワークス株式会社
- トレンドマイクロ株式会社
- 日本 RA 株式会社
- 日本電気株式会社
- 日本マイクロソフト株式会社
- PIPELINE株式会社
- 株式会社ベルウクリエイティブ
- 三井住友海上火災保険株式会社
- ミツフジ株式会社
- 株式会社ミルウス
- 株式会社ユビキタスAIコーポレーション
- 株式会社ラック
- ラピスセミコンダクタ株式会社
- Rambus Inc.,
- ワンビ株式会社

【賛助会員：20団体】

- IoTSecJP
- エッジプラットフォームコンソーシアム
- 株式会社N Cネットワーク
- NPO法人クライシスマップーズ・ジャパン
- 一般社団法人重要生活機器連携セキュリティ協議会
- 一般財団法人石炭エネルギーセンター
- 一般社団法人セキュアドローン協議会
- 中央コリドー高速通信実験プロジェクト推進協議会
- 一般社団法人データ流通推進協議会
- 一般財団法人日本データ通信協会
- 一般社団法人日本クラウドセキュリティアライアンス
- 一般社団法人日本スマートフォンセキュリティ協会
- 一般社団法人日本テレワーク協会
- 学校法人電子学園 日本電子専門学校
- NPO法人日本ネットワークセキュリティ協会
- 公益財団法人ハイパーネットワーク社会研究所
- 働き方改革支援コンソーシアム
- NPO法人北海道森林療法研究会
- モバイルコンピューティング推進コンソーシアム
- YRP研究開発推進協会

SCOPEへの取り組み

●委託研究内容

- ・セキュアIoTプラットフォーム協議会と中央大学研究開発機構で共同受託
- ・研究テーマ：「IoT デバイス認証基盤の構築と新AI 手法による表情認識の医療介護への応用についての研究開発」
- ・研究内容：

IoT、ビッグデータ、AIを支える情報セキュリティ基盤の構築を目指し、電子認証(真正性確認)を軸とした4階層(デバイス層、ネットワーク層、データ管理層、情報サービス層)に対し、研究開発/ビジネスモデル構築/社会的普及/ガイドライン・標準化の作成を図る。

基軸理念	階層・重点テーマ	各層の目的
真正性保証	情報サービス層 基盤理論構築	リーマン幾何学を用いた新 AI による、敵対学習による誤認識の防止・真正性の高い表情を認識する手法の確立。デバイス層と連携し、要介護施設等で実証実験。
	データ管理層 耐改竄性強化	情報漏洩・改竄防止の為に、論理式に対する暗号化状態処理手法・組織暗号の安全性・秘匿検索
	ネットワーク層 データ送信プロトコルの提案	送信デバイスや送信データの真正性の確保および送信デバイスの匿名性と特定・追跡性の両立が可能な認証方式の提案、および組織・個人・IoT を対象とする認証方式全体の枠組の提案
	デバイス層 IoT 基盤実装	重要デバイスへの電子認証の埋め込みと監視・見守りカメラへの実装

【2018年度成果】

- ・IoTデバイスへのPKI電子認証の基本コンセプト発表
 - ・論文：2018.11 信学技報 (IEICE Technical Report)
- ・IoT機器のライフサイクルにおいて想定される脅威、対策、評価方法を整理
 - ・2018年度： 企画・設計フェーズ(完了)
 - ・2019年度： 開発～製造～運用～廃棄フェーズ 作成



【2019年度活動予定】

- ・介護施設での実証実験に向け、カメラに対する認証の仕組みを実装し、以下のテストを実施
 - ・証明書ベースでのカメラの個体認証
 - ・管理コンソール上からの機器管理
 - ・撮影映像への署名およびデータ転送

AGENDA



- なぜ、IoT機器が狙われるのか？
- モノの認証により実現できること＝目的
- モノに求められるセキュリティ機能
- 重要IoT機器には認証が不可欠
- 「Trust Anchor」と「Root of Trust」
- IoT機器のライフサイクルマネジメント
- IoT機器の安全・信頼の課題
- IoT機器認証の検討課題

なぜ、IoT機器が狙われるのか？

常時接続



- 365日24時間接続可能

脆弱性



- 複数の攻撃ポイント
- 侵入が比較的容易
- セキュリティ対策が不十分な機器が多い

低コスト



- IoT機器のボット化はPCよりも攻撃の費用対効果が高い

管理者不在



- 未アップデート機器が多い
- アフターサービスが未熟な製品が存在
- 所有者スキルに依存

モノの認証により実現できること＝目的

トラストチェーンの形成



製造工程からの
トレーサビリティ

半導体～機器製造時に専用チップに安全に鍵を書き込みそのカギにつなぎ合わせ認証局から電子証明書を発行し、**デバイスのトレーサビリティを確保**



IoT機器の
長期瑕疵担保

証明書の長期更新とIoT機器に対する長期サポート供給など、製品出荷後の**IoT機器の安全なメンテナンス**



機器の
IoT化を支援

エコパートナーと連携し、IoT機器に対し鍵を配付するなどの**IoT基盤が不可欠**

重要IoT機器には認証が不可欠

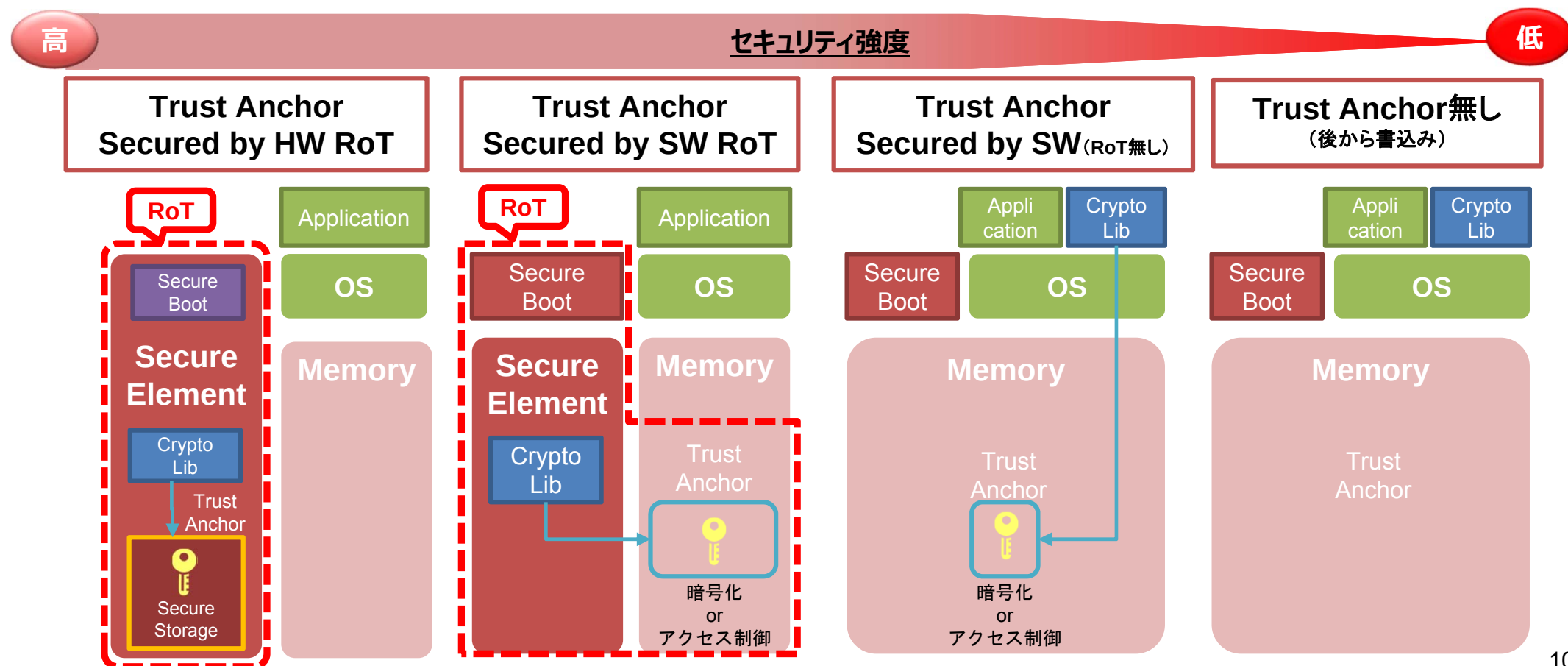
デバイスの製造時からソフト更新、廃棄まで「安全」であることが重要



全ての重要IoT機器へのPKI電子認証の導入が必要

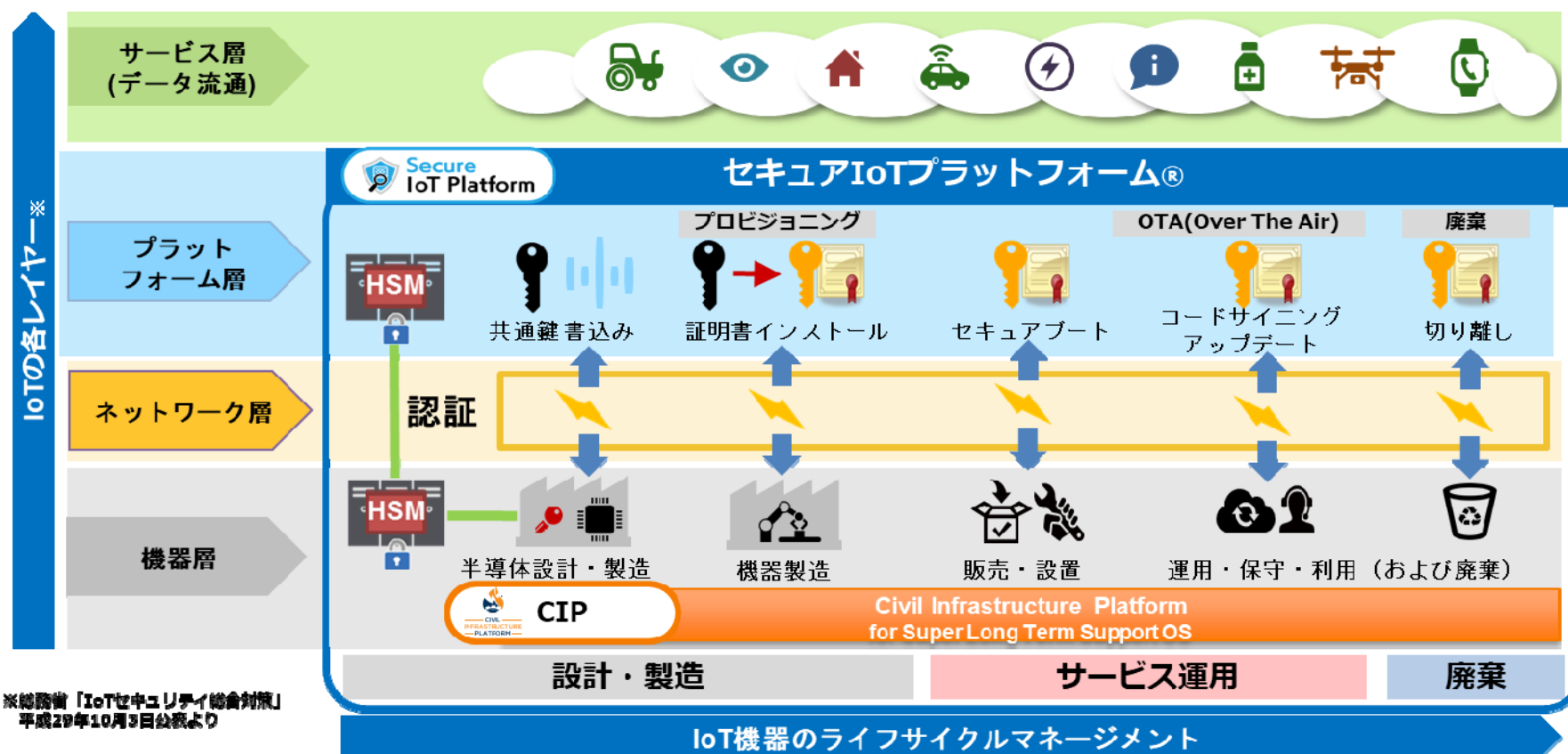
認証の実装方法とセキュリティ強度

求められるセキュリティ強度に応じて、
信頼の基点となる鍵(Trust Anchor)の格納方法(Root of Trust)を選択することが必要



IoT機器のライフサイクルマネジメント

PKIによる機器認証をベースに
「IoT機器の設計・製造」～「利用・保守・運用」～「廃棄」に至る
安全かつ確実なプロダクトライフサイクル管理を実現



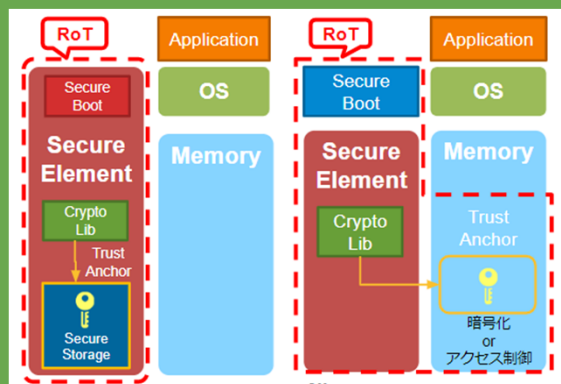
※総務省「IoTセキュリティ総合対策」
平成29年10月3日公表より

IoT機器の安全・信頼の課題

IoT機器の開発では、安全・信頼をどのように実現し提供するかがポイントに

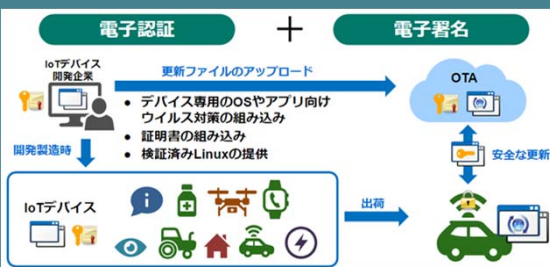
Root of Trust

- サイバー攻撃対策
- 電子証明書・鍵の管理
- 信頼の担保



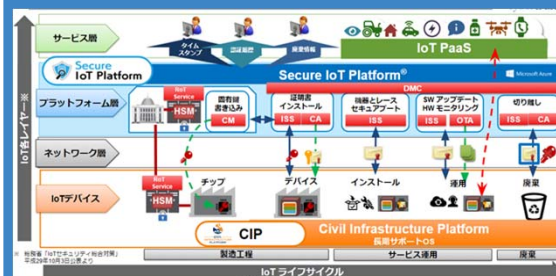
OTA・デバイス管理

- 安全なOTAの提供
- デバイスの集約管理
- 認証の仕組み



ライフサイクル管理

- 製品出荷~破棄の管理
- サプライチェーン
- 長期保守



IoT機器認証の検討課題

【課題シナリオ】すべてのIoT機器に認証の仕組みを導入するためには

■導入の課題

- ✓ 単価（コスト）の上昇
- ✓ サービス提供事業者の事業継続性
- ✓ 大量のIoT機器の管理
 - ・ 電子証明書の発行スピードの課題
 - ・ CRL、OCSPの大量問合わせの課題
 - ・ DBの検索性（スピード、アクセスログetc）

■普及の課題

- ✓ 法的根拠
 - ・ 電子署名法における「認定認証業務」相当の認定制度の検討
- ✓ プラットフォーム化／マルチテナント／標準化
 - ・ 誰が作っても同じセキュリティ強度やクオリティが担保できるか
 - ・ 公的資金による普及支援
 - ・ 国際連携の中で相互接続性が保てるか
- ✓ メーカー側のメリットの整理
 - ・ 費用対効果
 - ・ ユーザー（利用者）からの要求なのか
 - ・ 国際競争力につながるのか