IPA Better Life with IT

Embedded Technology WEST 2017 IoT Technology WEST 2017

# IoT機器や関連システムに求められる安全安心のための機能と機能要件

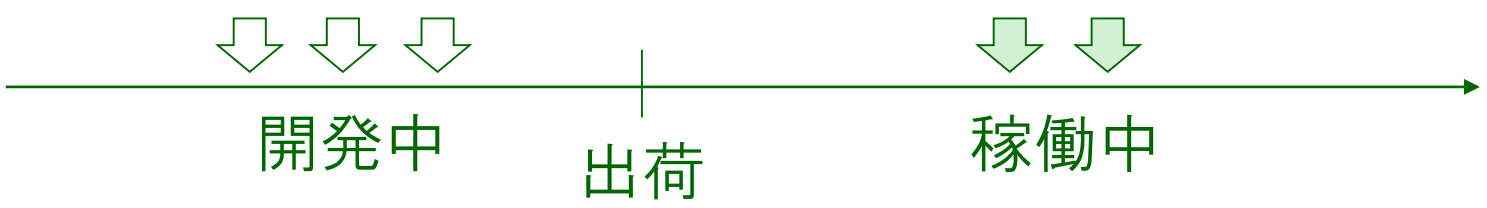
## 「『つながる世界の開発指針』の実践に向けた手引き」の紹介

森崎　修司

IPA IoT高信頼化機能検討ワーキング・グループ
名古屋大学 大学院情報学研究科

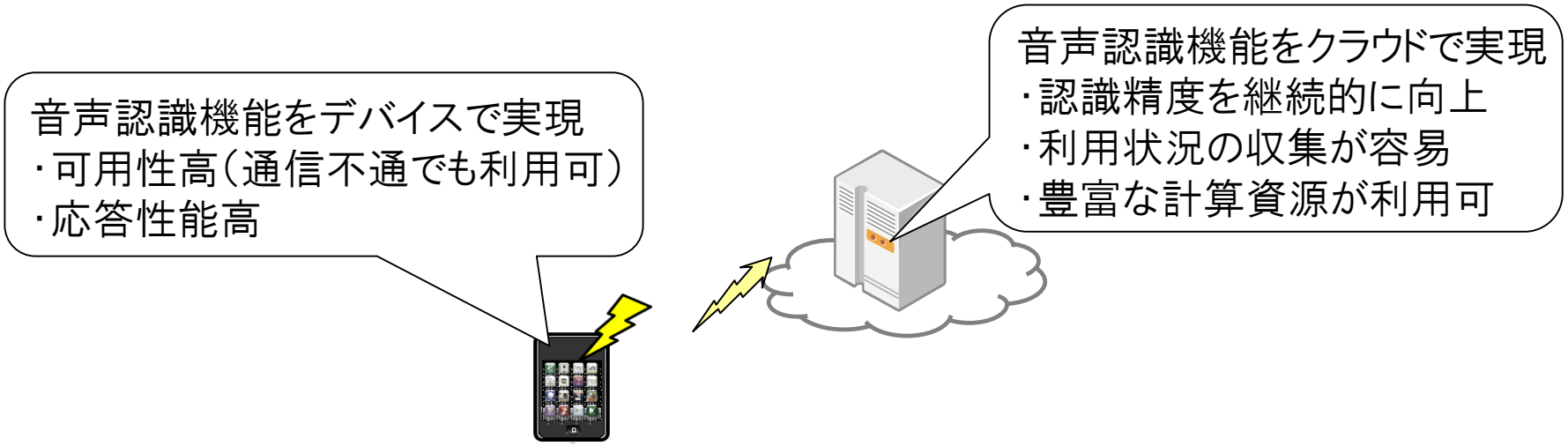
# ソフトウェアやサービスの変化

- 出荷後も継続的に更新し満足度や品質を高めることが増えている分野もある。
  - ネットワークの普及と低廉化により利用状況の収集と出荷後のソフトウェア更新が容易になった。
  - フィードバックを反映しながら、粒度の小さい機能(Minimum Marketable Feature)を継続的に更新する方法が現れた。
- ソフトウェアが付加価値の中心を担う分野もある。
  - 行動、観測データの収集コストが下がり、ビジネス活用が現実的になりつつある。
  - 高度な機械学習により、これまで難しかったことが予測、自動化できる部分がある。



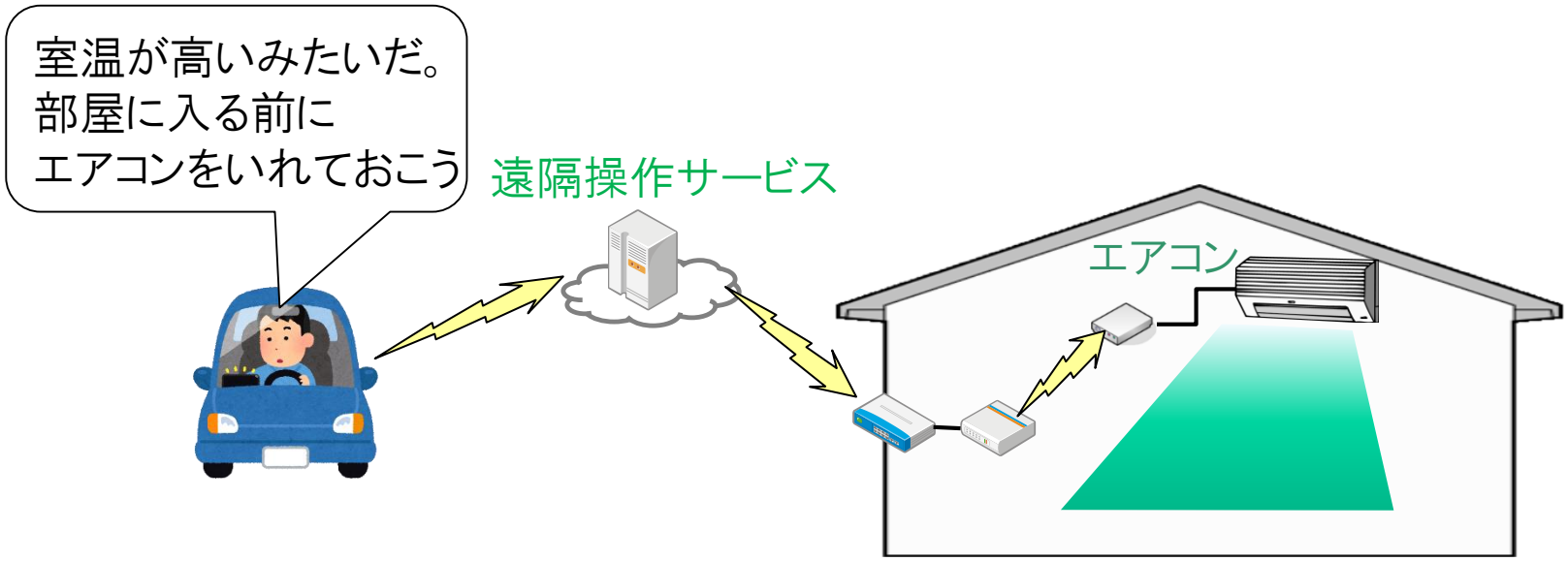
# ネットワークの普及と低廉化

- 機器・システムをネットワークでつなげられるようになった。
  - 移動しなくても機器（センサー、デバイス）とリアルタイムに情報を共有できるようになった。
- ネットワークにより機能配置の自由度が高まった。
  - デバイスで実現
  - サーバサイド（クラウド上）で実現



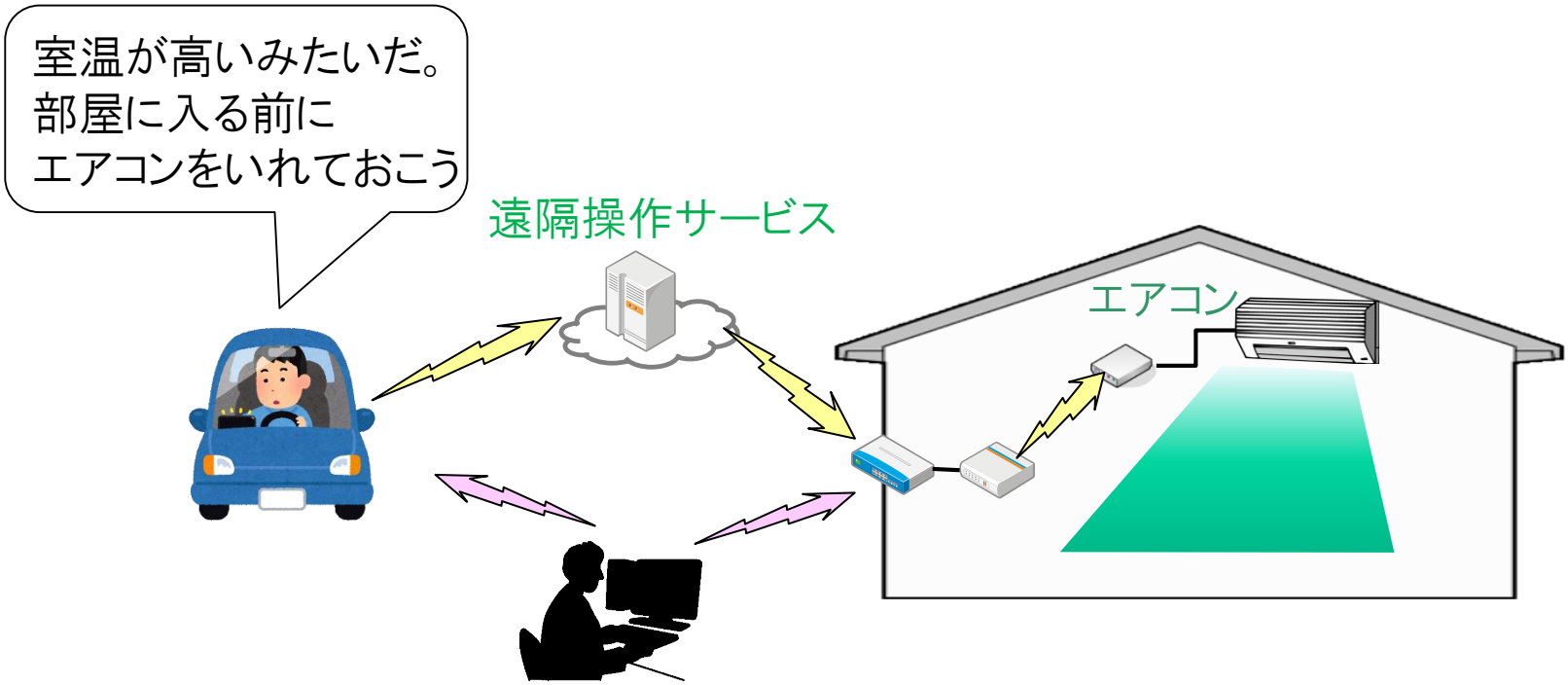
# IoT(Internet of Things)時代の到来

- 機器･システムが相互につながることが付加価値の一つとなる。



# IoTへの対応の課題

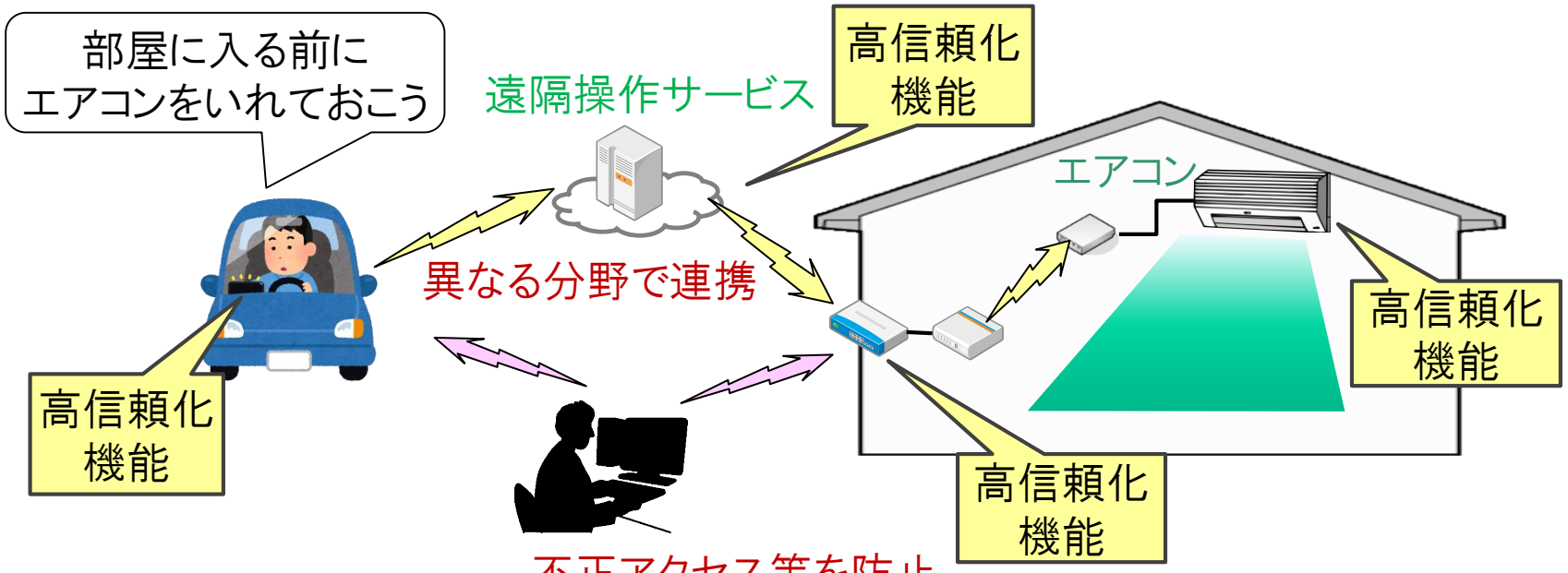
- 単純につなぐだけでは様々なリスクがある。




悪意ある攻撃者がエアコンを
勝手に制御したり、偽の室温を
提示したりする可能性がある。

# IoT高信頼化機能

- IoT機器や関連システムに求められる安全安心のための機能をIoT高信頼化機能と呼ぶ。



# 機能レベルの公開情報の不足

- 機能定義や機能配置といった具体的な情報は少ない。
- セキュリティ中心でセーフティへの言及は少ない。

具体性

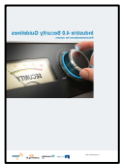
▲

低

IPA/SEC
つながる世界の開発指針
（2016年3月）

IoT推進コンソーシアム
IoTセキュリティガイドライン
（2016年7月）

CCDS
製品分野別セキュリティ
ガイドライン（2016年6月）



VDMA（独）
Industrie 4.0 Security
Guidelines
（2017年3月）

CSA（米）
Security Guidance for
Early Adapters of the
Internet of Things（2015
年4月）

GSMA（英）
IoT Security Guidelines
（2016年2月）

JNSA
コンシューマ向けIoTセキュリティガイド
（2016年8月）

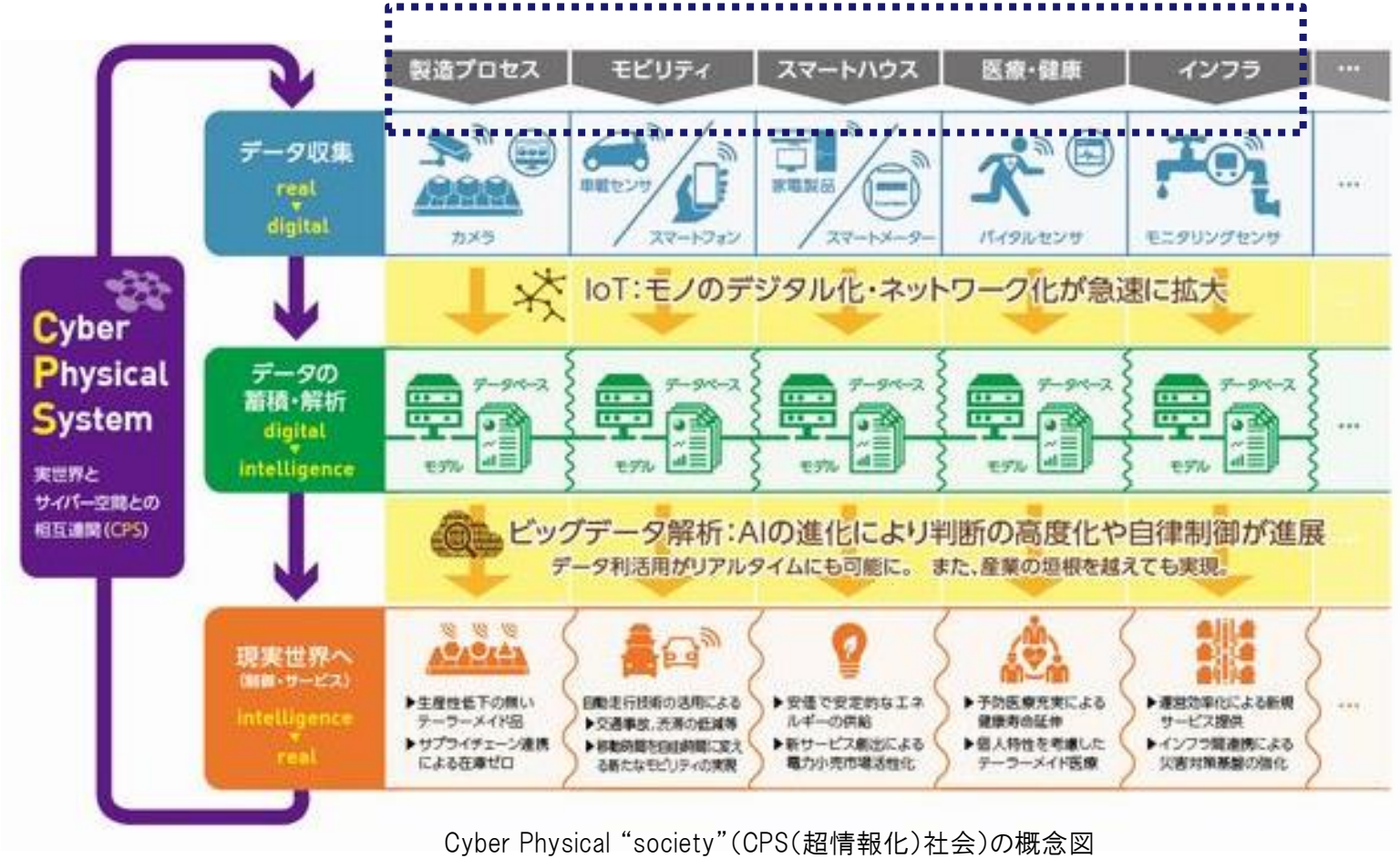
IIC（米）
Industrial Internet Security
Framework
（2016年9月）

高

時間

# 分野間連携の情報不足

- 利便性向上やコスト削減のために分野を横断した連携へ拡大の見込みがあるがそうした情報は少ない。




Cyber Physical “society”(CPS(超情報化)社会)の概念図
【出典】平成27年4月　産業構造審議会 商務流通情報分科会 情報経済小委員会 中間とりまとめ」を元に追記

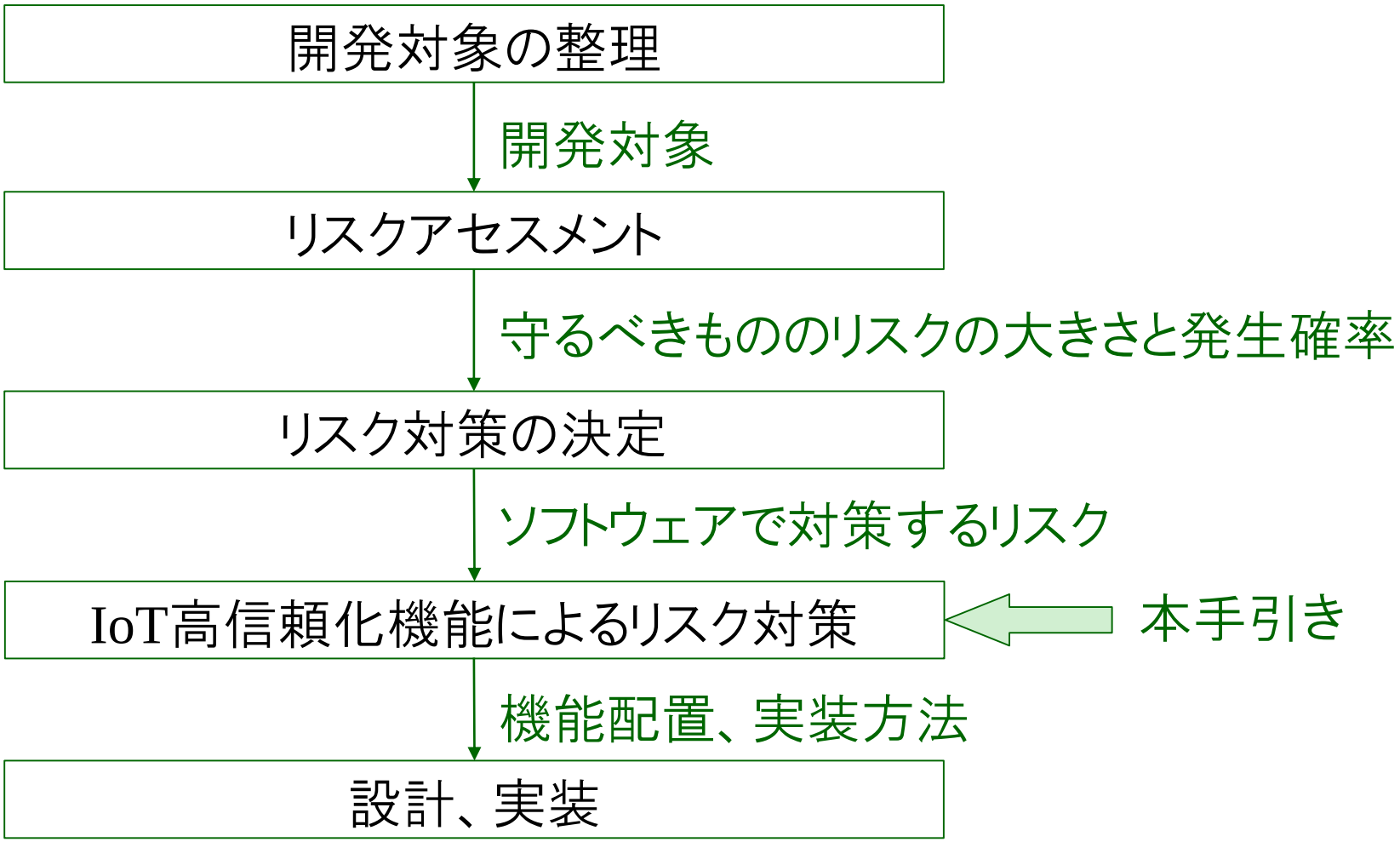
# 背景

- つながる時代（IoT時代）の到来
  - 各種機器（デバイス、センサー）がネットワークにつながり新しいサービスが生み出される。
    → つながらないことで競争力を損なう。
- つながることによるリスク
  - 単につながるようにするだけでは、正当な権限がない者により情報が参照できたり制御できたりする可能性がある。
    → 利用者の安全安心への配慮不足が競争力を損なう。
- 設計情報の不足
  - 設計、実装レベルの情報、分野間連携を意識した情報が少なく、構成見直しや大きな作り直しにつながる可能性がある。
    → 利便性向上やコスト低減が難しくなり競争力を損なう。

# 『つながる世界の開発指針』の実践に向けた手引き

- 「つながる世界の開発指針」を具体化した。
- 背景
  - つながる時代（IoT時代）の到来
  - つながることによるリスク
  - 公開情報の不足
- 内容
  - 安全安心を提供する機能（IoT高信頼化機能）を紹介する。
  - 運用フェーズごとに機能を対応づけ、機能配置を考慮することにより開発者が自身の開発に役立てやすくする。
  - 将来見込まれる分野間連携を意識した設計、実装をイメージしやすくする。

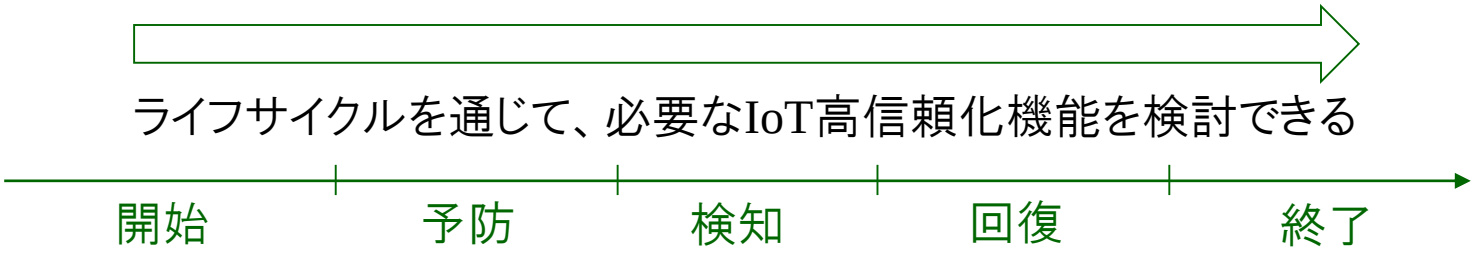
# 手引き活用の全体像


開発対象の整理
開発対象
リスクアセスメント
守るべきもののリスクの大きさと発生確率
リスク対策の決定
ソフトウェアで対策するリスク
IoT高信頼化機能によるリスク対策
本手引き
機能配置、実装方法
設計、実装

# 機器･システムのライフサイクル

- 機器･システムの開始、予防、検知、回復、終了までのライフサイクルを軸に要件、機能要件、機能を提示している。

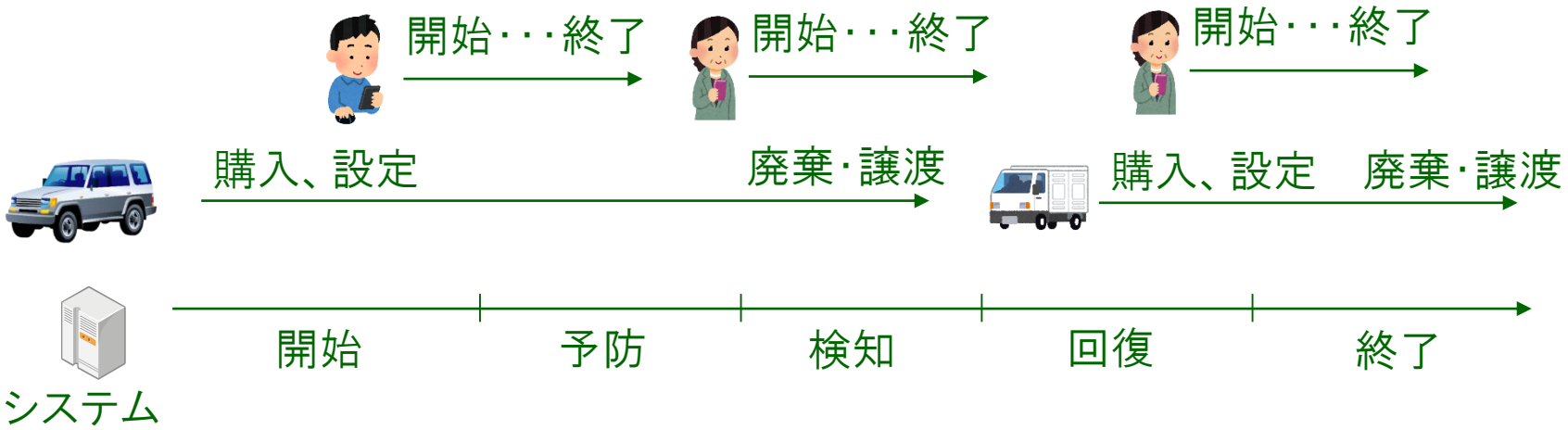
| ライフサイクル | 要件 |
|---|---|
| 開始 | 導入時や利用開始時に安全安心が確認できる |
| 予防 | 稼働中の異常発生を未然に防止できる |
| 検知 | 稼働中の異常発生を早期に検知できる |
| 回復 | 異常が発生しても稼働の維持や早期の復旧ができる |
| 終了 | 利用終了、システム･サービス終了後も安全安心が確保できる |



# ライフサイクルの多層化

- ライフサイクルが多階層にわたることもあり、それぞれにおいて考慮が必要になる。

レンタカーの例



# ライフサイクルとIoT高信頼化機能の対応

| ライフサイクル | | 機能要件 | 機能 |
|---|---|---|---|
| 開始 | 導入時や利用開始時に安全安心が確認できる | 初期設定が適切に行われ、その確認ができる | 1, 2 |
| | | サービスを利用する時に許可されていることを確認できる | 3, 4 |
| 予防 | 稼働中の異常発生を未然に防止できる | 異常の予兆を把握できる | 5, 6, 7, 8, 9 |
| | | 守るべき機能･資産を保護できる | 4, 5, 6, 10 |
| | | 異常発生に備えて事前に対処できる | 11 |
| 検知 | 稼働中の異常発生を早期に検知できる | 異常発生を監視･通知できる | 12,13 |
| | | 異常の原因を特定するためのログが取得できる | 5, 6 |
| 回復 | 異常が発生しても稼働の維持や早期の復旧ができる | 構成の把握ができる | 14 |
| | | 異常が発生しても稼働の維持ができる | 8, 15, 16, 17 |
| | | 異常から早期復旧ができる | 11, 18, 19, 20 |
| 終了 | 利用終了、システム･サービス終了後も安全安心が確保できる | 自律的な終了や一時的な利用禁止ができる | 18, 21, 22 |
| | | データ消去ができる | 23 |

# 手引きに記載しているIoT高信頼化機能

| | | | |
|---|---|---|---|
| 1 | 初期設定機能 | 13 | 状態可視化機能 |
| 2 | 設定情報確認機能 | 14 | 構成情報管理機能 |
| 3 | 認証機能 | 15 | 隔離機能 |
| 4 | アクセス制御機能 | 16 | 縮退機能 |
| 5 | ログ収集機能 | 17 | 冗長構成機能 |
| 6 | 時刻同期機能 | 18 | 停止機能 |
| 7 | 予兆機能 | 19 | 復旧機能 |
| 8 | 診断機能 | 20 | 障害情報管理機能 |
| 9 | ウイルス対策機能 | 21 | 操作保護機能 |
| 10 | 暗号化機能 | 22 | 寿命管理機能 |
| 11 | リモートアップデート機能 | 23 | 消去機能 |
| 12 | 監視機能 | | |

# IoT高信頼化機能の記載例

## (9) ウイルス対策機能

| | |
|---|---|
| 目的 | ウイルス感染の被害を防止する。 |
| 説明 | ウイルス対策には、検出(侵入、実行、潜伏を含む)、駆除がある。検出には以下のような方式がある。<br>・ ホワイトリスト方式<br>– 特にリソースの少ない IoT 機器の場合においては、登録されたソフトウェアのみ実行を許可することで、未知のウイルスの実行を防止する。<br>・ ブラックリスト方式<br>– ウイルスチェックには、既知のウイルスをパターンファイルに登録し侵入、実行、潜伏を検出する。<br>ブラックリスト方式は、リソースが少ない場合には実装が難しいことが想定される。 |
| 参考 | 制御システム向けの端末防御技術「ホワイトリスト型ウイルス対策」とは？<br>http://monoist.atmarkit.co.jp/mn/articles/1404/07/news004.html |

IoTについて考慮した事項

各機能の説明は簡潔にまとめ、関連情報を記載

## (12) 監視機能

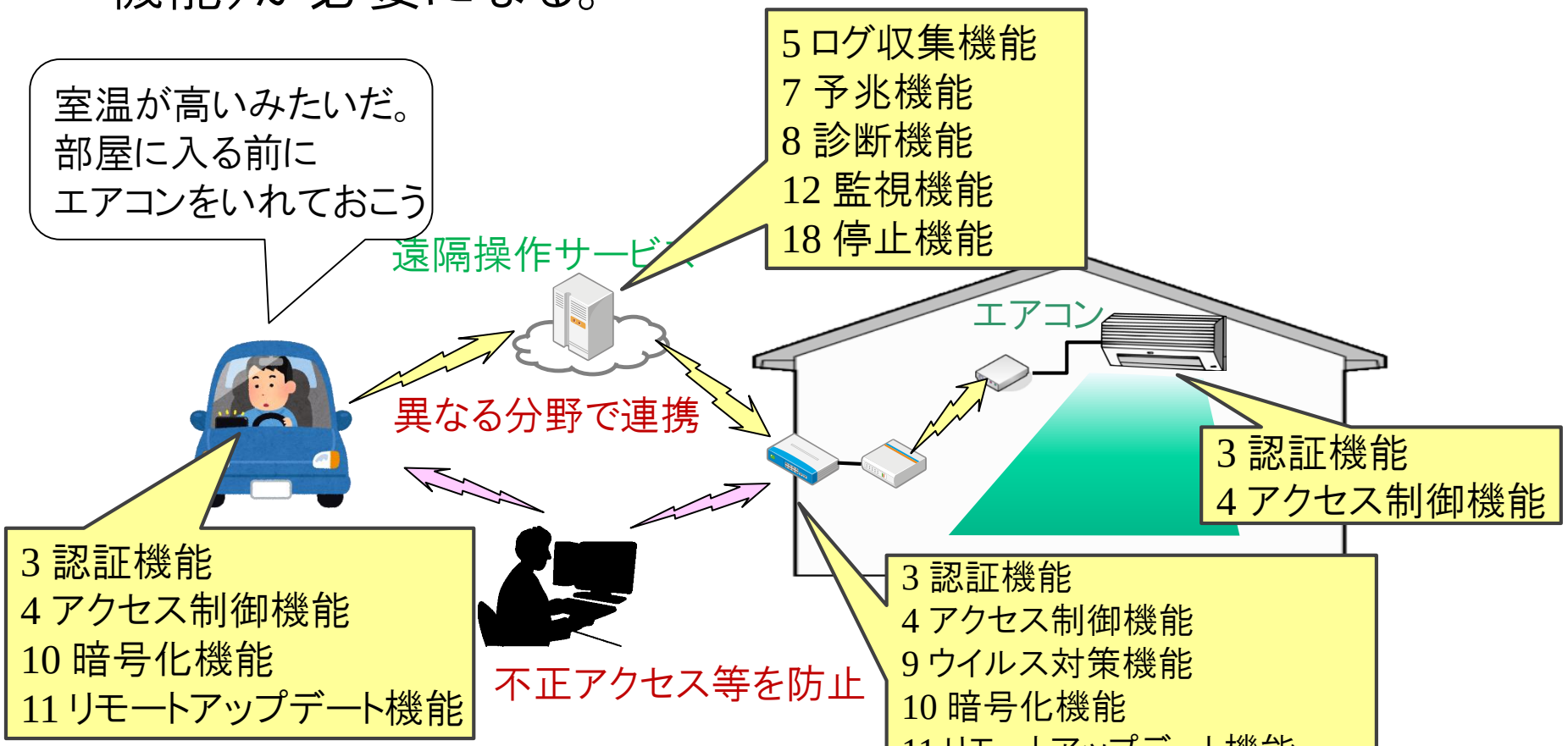
| | |
|---|---|
| 目的 | 機器・システムの異常を検知する。 |
| 説明 | 監視機能には以下のような機能がある。<br>・ 異常の検知機能<br>– 障害/故障の検知(ログ分析含む)<br>– セキュリティ異常の検知(ログ分析含む)<br>– 制御の競合の検知　等<br>・ 検知した異常の通知機能 |
| 参考 | |

セキュリティだけではなく、セーフティやリライアビリティに関する事項も含む

ワーキング・グループでのユースケース分析から明らかになった点も記載

# IoT高信頼化機能の実装例

- 利用者の安全安心を確保するための機能（IoT高信頼化機能）が必要になる。



# 手引きの検討体制

- 異なる分野から集められた専門委員からなるワーキング・グループ(IoT高信頼化検討WG)を設置して検討
  - 分野を横断する利用シーン（ユースケース）を具体的にあげ、機能・要件を検討
  - 活動期間：2016年7月～2017年3月

| 役割 | 氏名 | 所属 | 専門分野 |
|---|---|---|---|
| 主査 | 森崎 修司 | 国立大学法人名古屋大学 | |
| 委員 | 伊藤 公祐 | 一般社団法人重要生活機器連携セキュリティ協議会(CCDS) | 生活機器 |
| 委員 | 鹿妻 洋之 | 一般社団法人電子情報技術産業協会（JEITA） | 健康器具 |
| 委員 | 柘植 晃 | YRP研究開発推進協会 /一般社団法人WSN-ATEC | Wi-SUN |
| 委員 | 辻 和隆 | 一般社団法人日本電機工業会 | 分散型エネルギー |
| 委員 | 中垣 良夫 | 株式会社デンソー | 自動車 |
| 委員 | 村上 隆史 | 一般社団法人エコーネットコンソーシアム | HEMS |
| 委員 | 吉府 研治 | 一般社団法人情報通信ネットワーク産業協会（CIAJ）/<br>日本電気株式会社 | ネットワークセキュリティ |

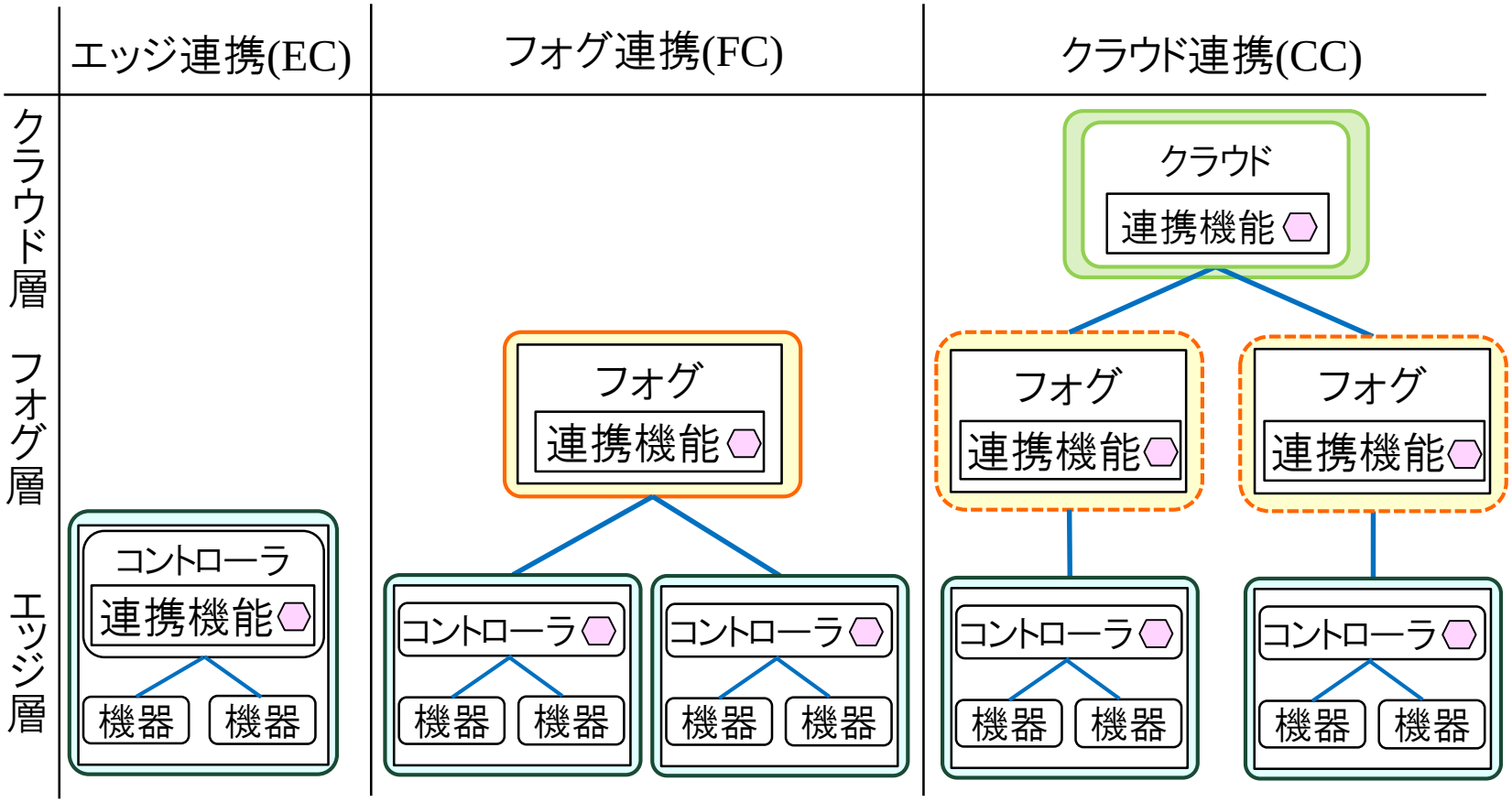
# 分野間連携のユースケース

- 現状実現できるものや今後想定されるものから、異なる分野にまたがる5つのユースケースを選び、WGで議論した。
- ユースケースによっては、複数の連携モデルの要素を含むことが分かった。（表中の「○」と「◎」）

| ユースケース | | EC | FC | CC | 補足説明 |
|---|---|---|---|---|---|
| 1 | 車両と住宅の連携 | | | ◎ | リアルタイム性は要求されないのでCCモデル |
| 2 | VPPと分散型電源監視サービスとの連携 | ○ | | ◎ | HEMSサーバ機能がクラウド上にあるモデルと需要家機器内にあるモデルがあり前者をCCモデルとして選定 |
| 3 | 宅内機器連携 | ◎ | | | HEMSのデバイスやコントローラ間の連携 |
| 4 | 戸締り競合制御 | ◎ | ○ | ○ | ホームGW／エッジサーバ内の複数の制御ソフト間で競合解決 |
| 5 | 産業ロボットと電力管理の連携 | ○ | ◎ | | 複数のサービスを連携し、判断の応答性が重視されるフォグ連携システムとして選定 |

# ユースケースで想定した連携モデル

- ユースケースの議論において3種類の連携モデルを想定して議論した。



# まとめ

- 「『つながる世界の開発指針』の実装に向けた手引き」を紹介した。
  - 安全安心を提供する機能（IoT高信頼化機能）
  - ライフサイクルと機能要件、機能の対応づけ
  - 分野間連携を想定したユースケース
  - ダウンロード: http://www.ipa.go.jp/sec/reports/20170508.html
- 「つながる世界の開発指」とあわせて、活用ください。