IoTの高信頼化機能を解説！

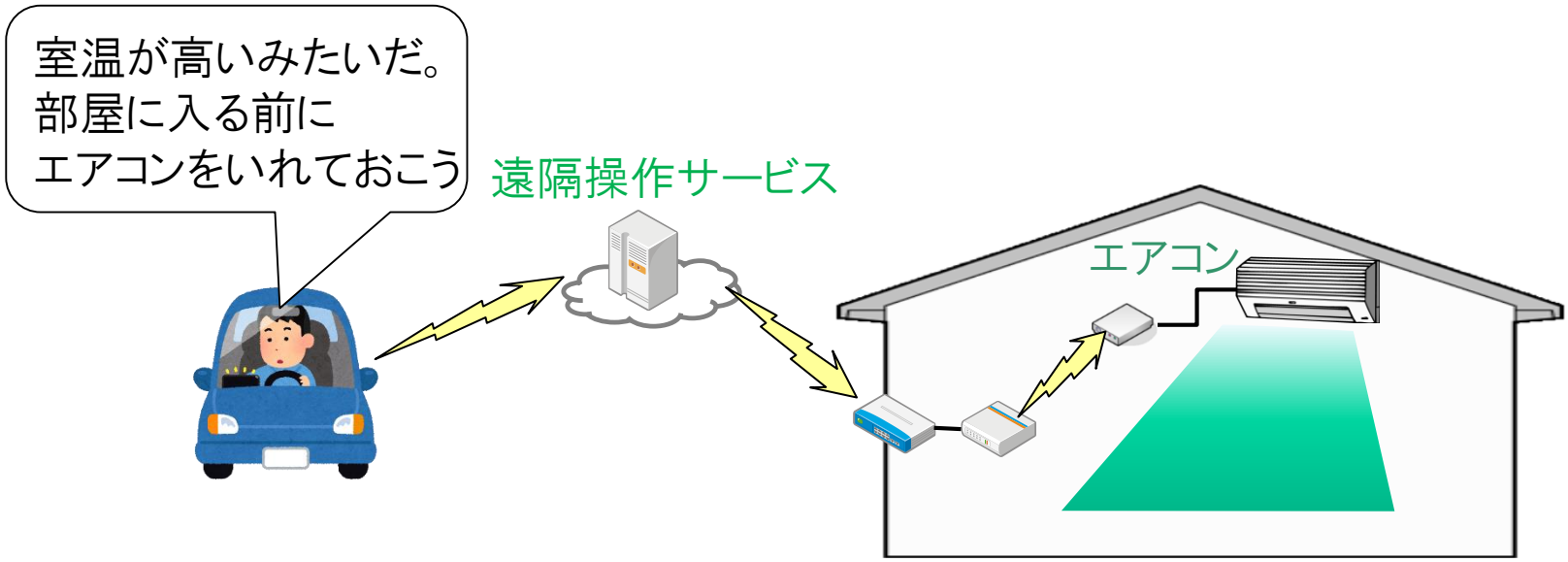
「『つながる世界の開発指針』の実践に向けた手引き」の紹介

森崎　修司

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

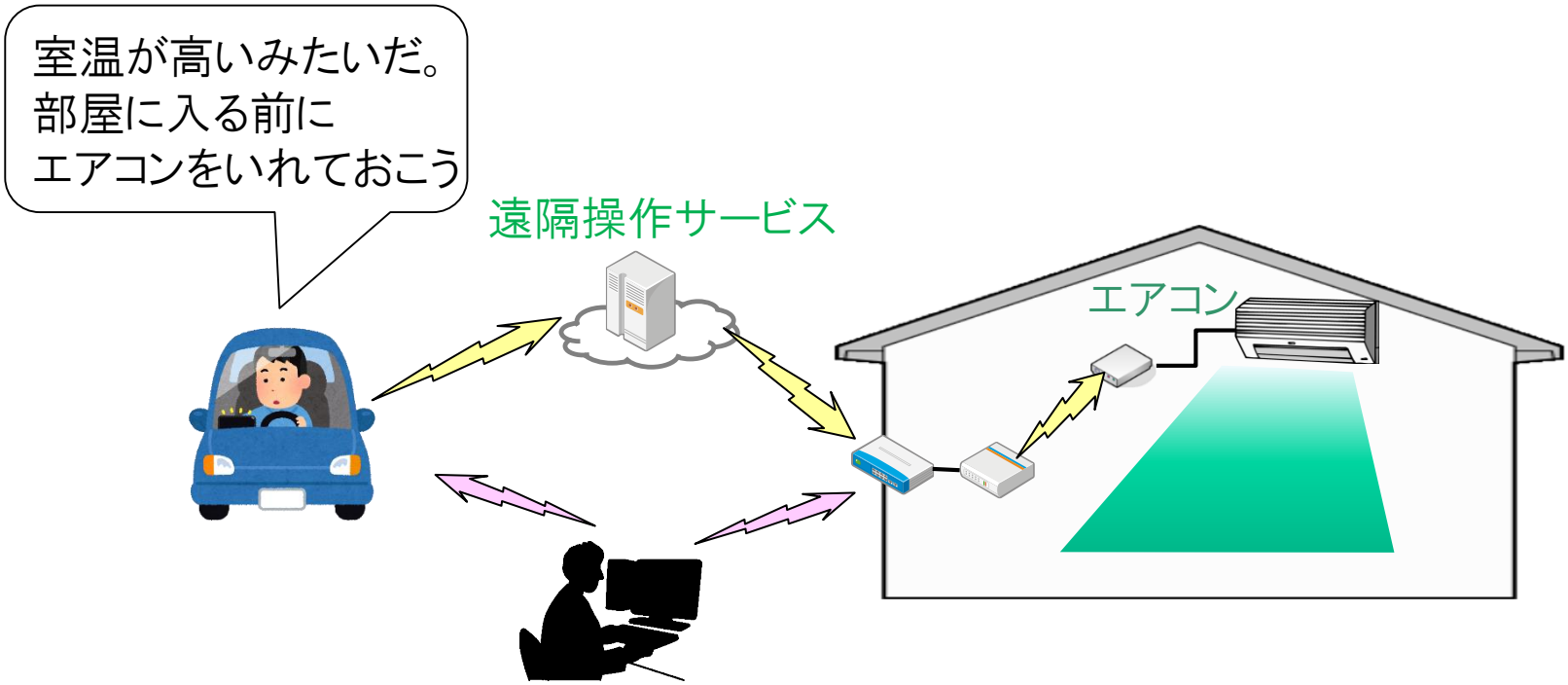
IoT(Internet of Things)の普及

- 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りつつある。



IoTへの対応の課題

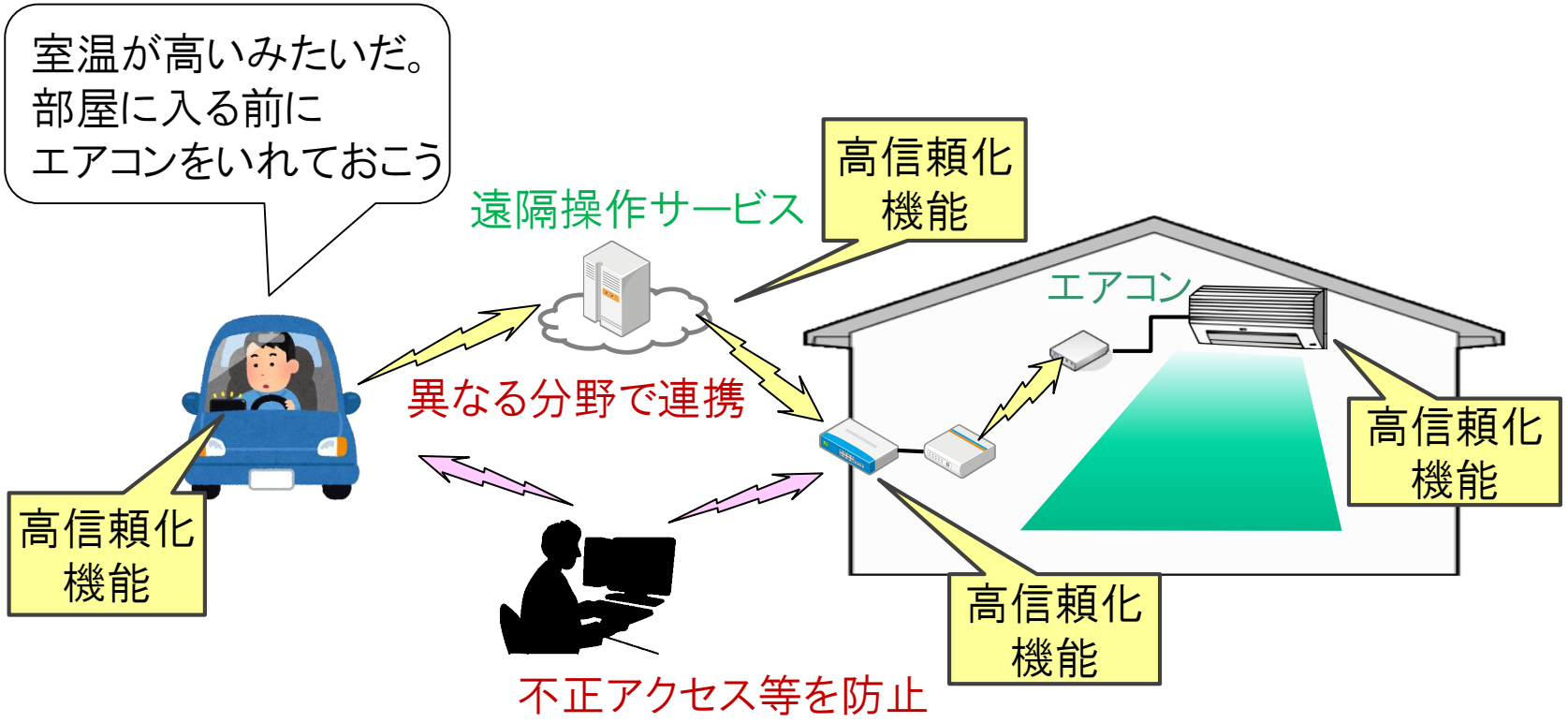
- 単につなぐだけでは、様々なリスクがある。



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。

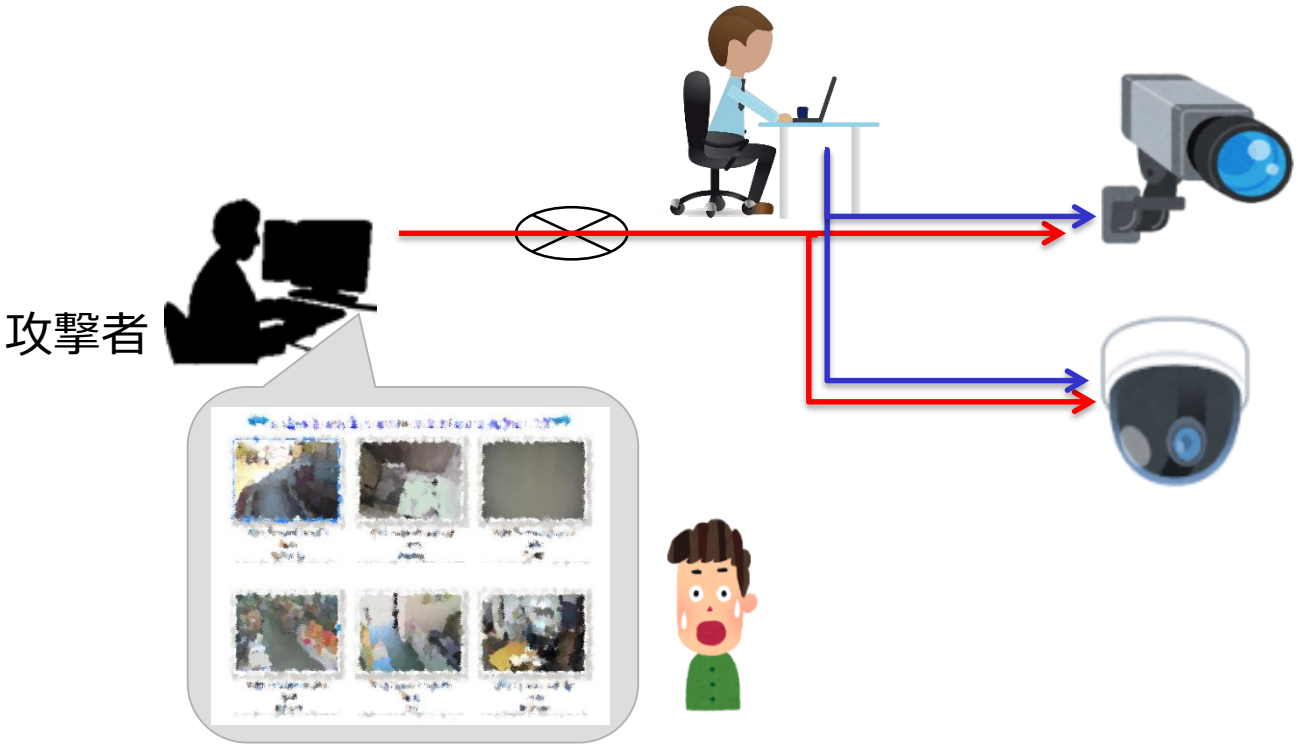
IoT高信頼化機能

- 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。



つながることによるリスクの例1

- カメラの映像が正当な権限を持たなくても参照できていた。
  - 工場出荷設定のままWi-Fiを通じてインターネットに接続
  - セキュリティ対策が不十分な日本国内の多数の監視カメラの映像が海外のインターネット上に公開されていた。



名古屋大学 NAGOYA UNIVERSITY

【出典】「経済産業省の取組とIoTセキュリティガイドラインVer1.0の概要」、経済産業省

つながることによるリスクの例2

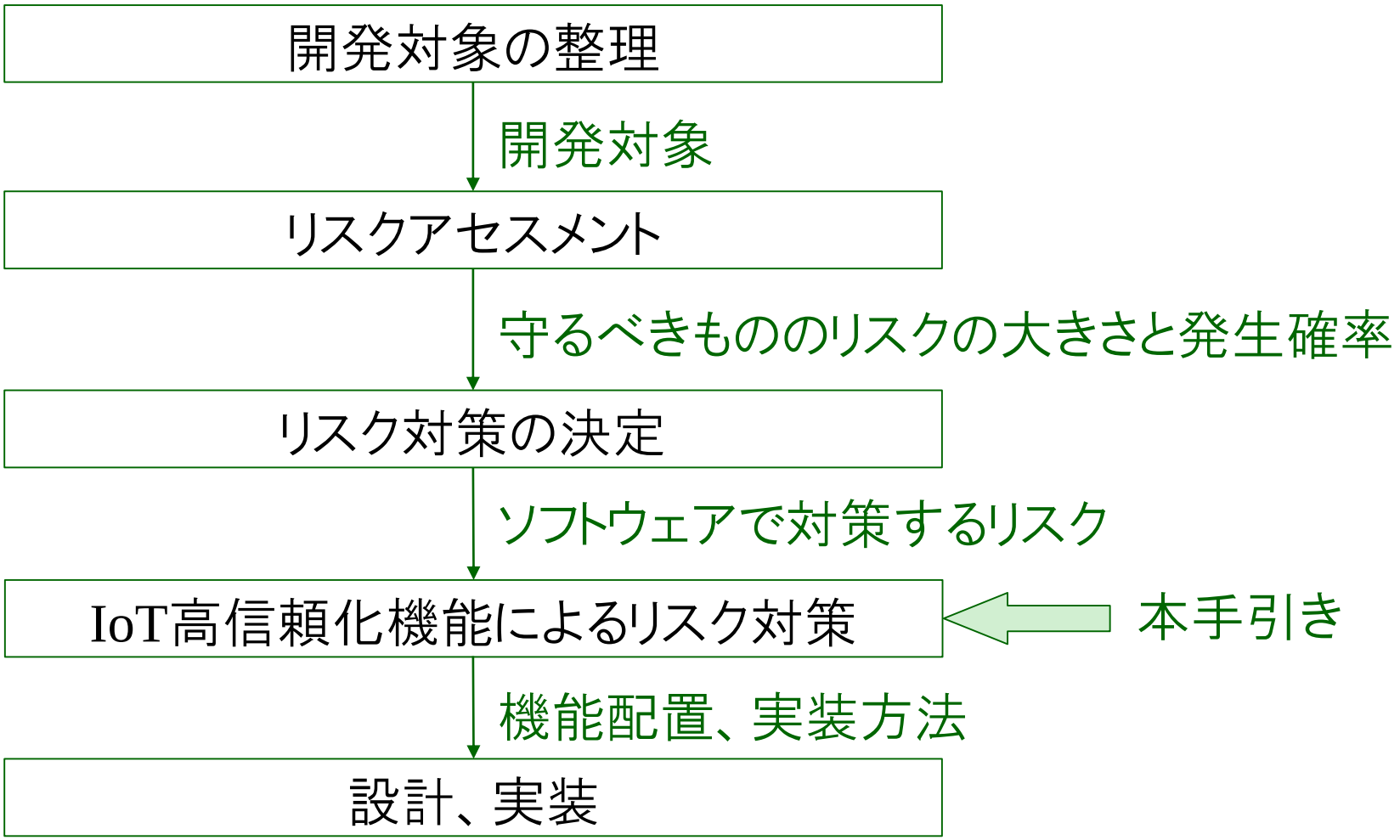
- カーナビ経由でハンドル、ブレーキを含む制御を奪取できていた。
  - 携帯電話網経由で遠隔地から操作できた。
  - 140万台に及ぶリコールを実施。

【出典】「経済産業省の取組とIoTセキュリティガイドラインVer1.0の概要」、経済産業省

『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の増加
  - 設計・実装レベルの公開情報の不足
- 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。

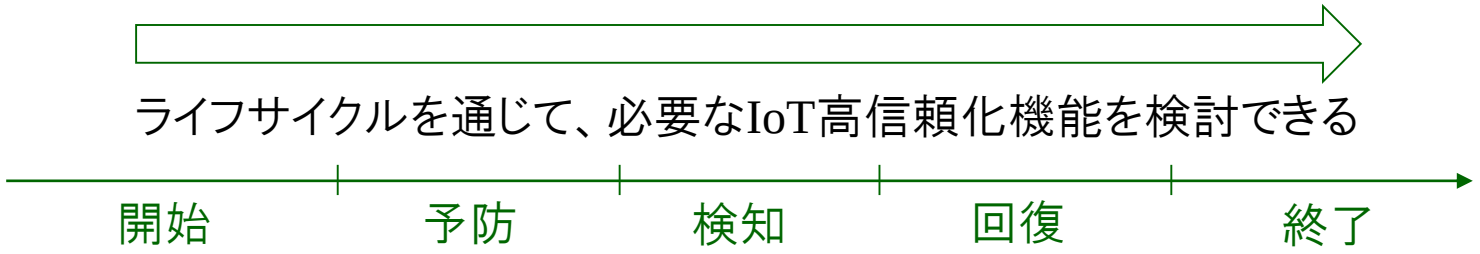
手引き活用の全体像


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

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。 ・ ホワイトリスト方式 – 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。 ・ ブラックリスト方式 – 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。 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？ 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。 ・ 異常の検知機能 – 障害/故障の検知(ログ分析含む) – セキュリティ異常の検知(ログ分析含む) – 制御の競合の検知　等 ・ 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

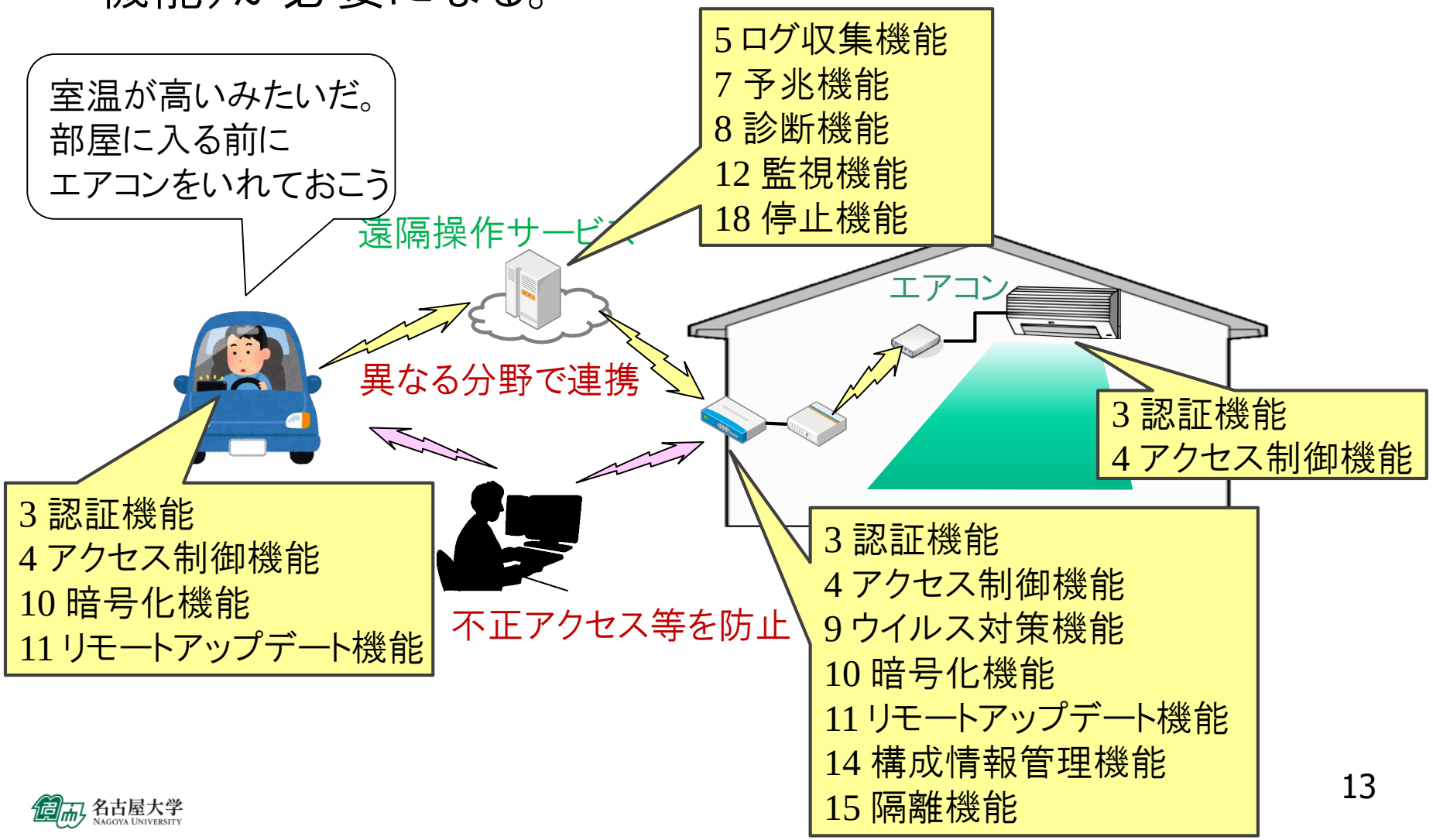
ワーキング・グループでのユースケース分析から明らかになった点も記載

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

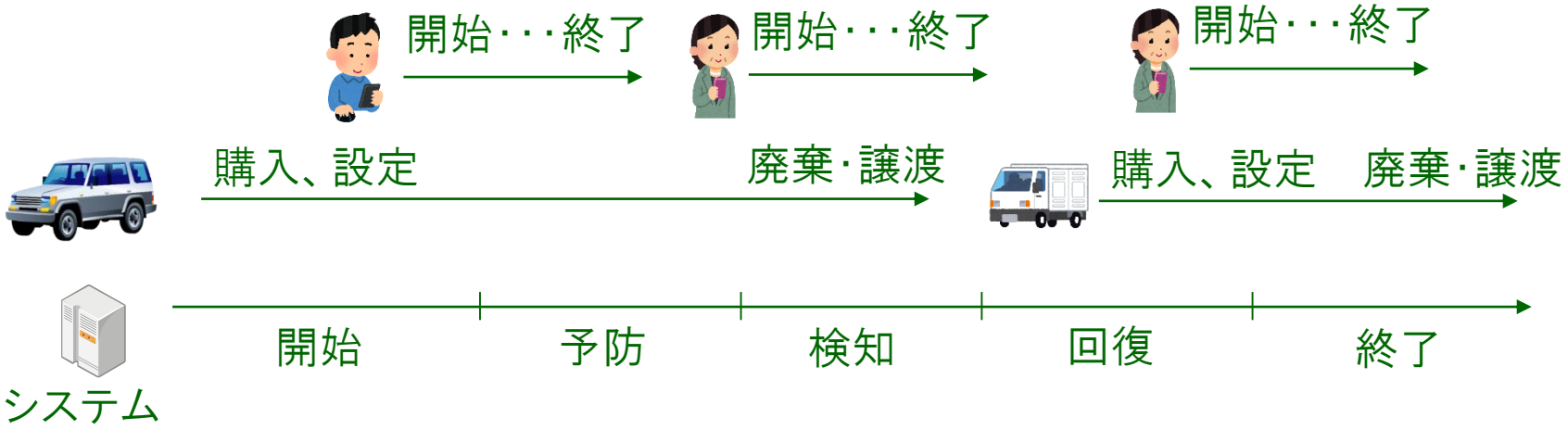
- 利用者の安全安心を確保するための機能（IoT高信頼化機能）が必要になる。



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



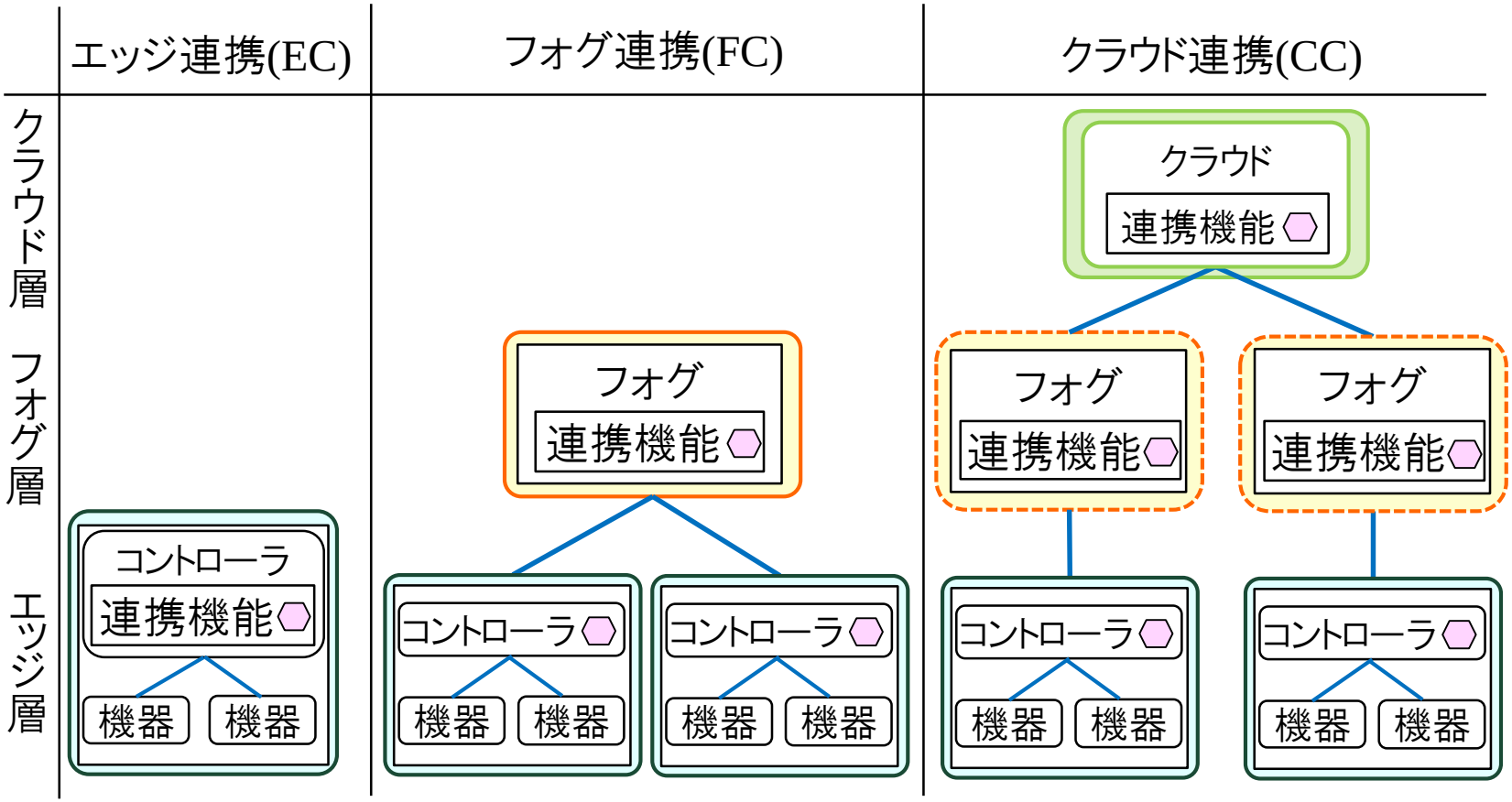
分野間連携のユースケース

- 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「〇」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	〇		◎	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	◎	〇	〇	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	〇	◎		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

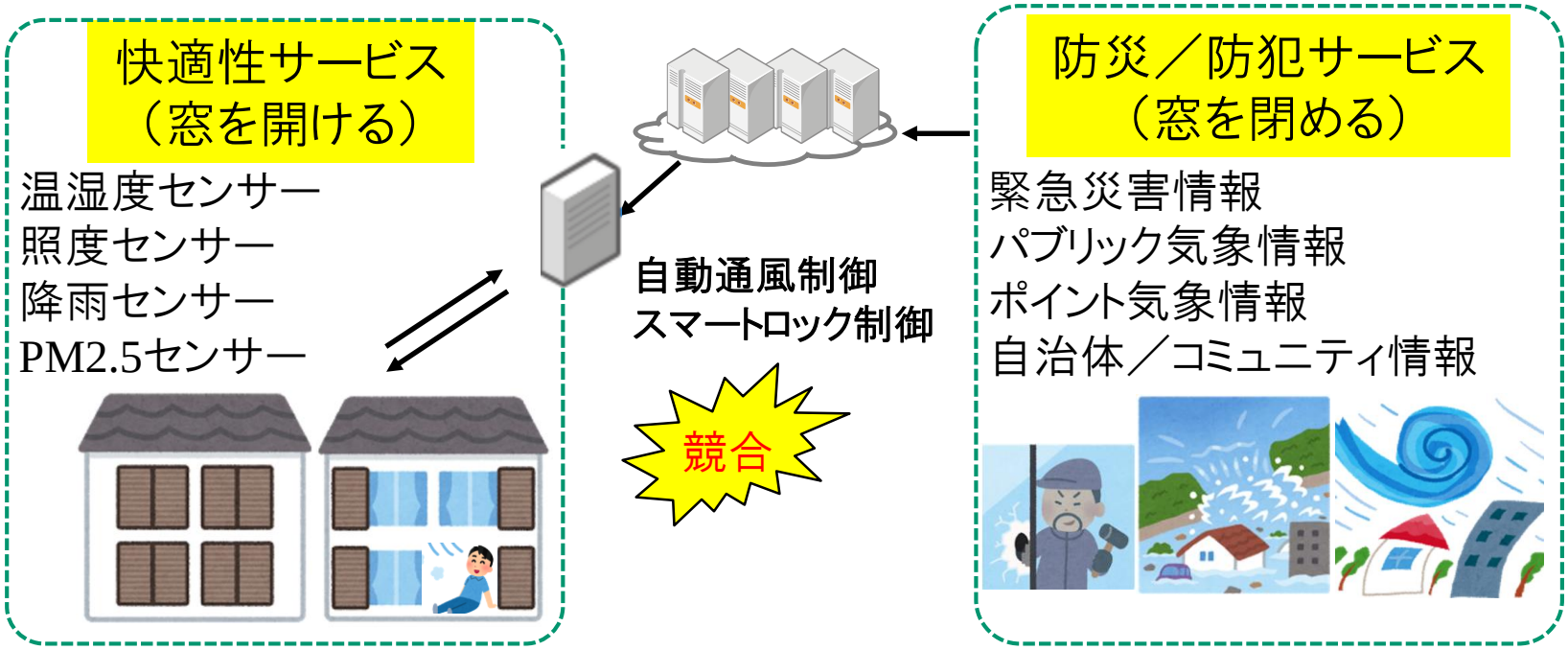
ユースケースで想定した連携モデル

- 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。



ユースケースの例: 戸締り制御の競合

- 宅内における快適性制御のための自動通風システムと緊急災害、防犯システムとの競合
- 想定される脅威/被害：制御ロジックが競合し安全性が損なわれる



窓の開閉に関する競合検知が必要になる

まとめ

- IoT時代の脅威とリスクを紹介した。
- IoT高信頼化機能を紹介した。
  - 安全安心を提供する機能
  - 機能の活用例
  - 詳細は「『つながる世界の開発指針』の実践に向けた手引き」をご覧ください。
    http://www.ipa.go.jp/sec/reports/20170508.html よりダウンロードできます。