IoTの安全・安心の実現に向けた開発の重要ポイント！

～つながる世界の開発指針の概説と展開活動の紹介～

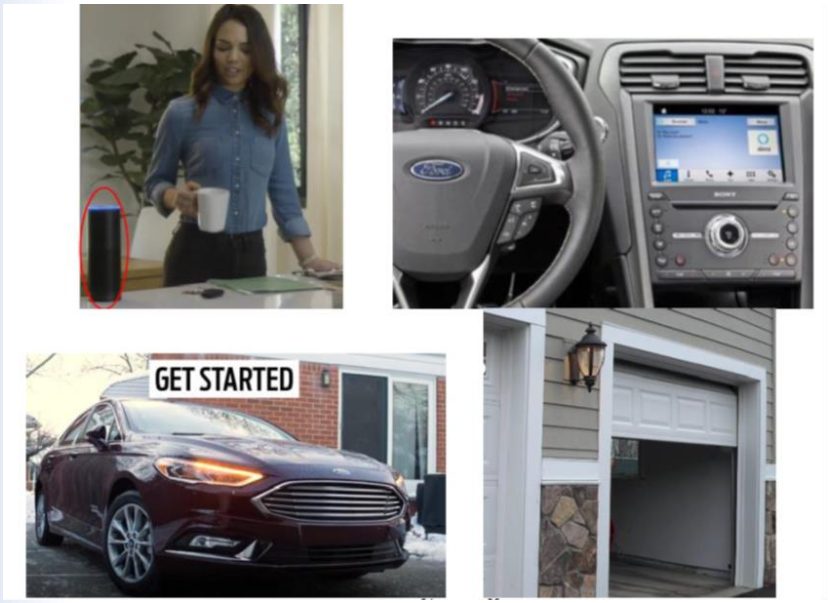
独立行政法人情報処理推進機構（IPA)
社会基盤センター　産業プラットフォーム部
調査役　宮原 真次

IoT/CPSの事例

■ 事例１）自動車と住宅の連携

・車内から自宅の玄関照明の点灯やガレージドアの開閉、スマート家電の操作

・自宅から車のエンジン始動やドアの施錠・開錠、燃料残量チェック、エアコン操作

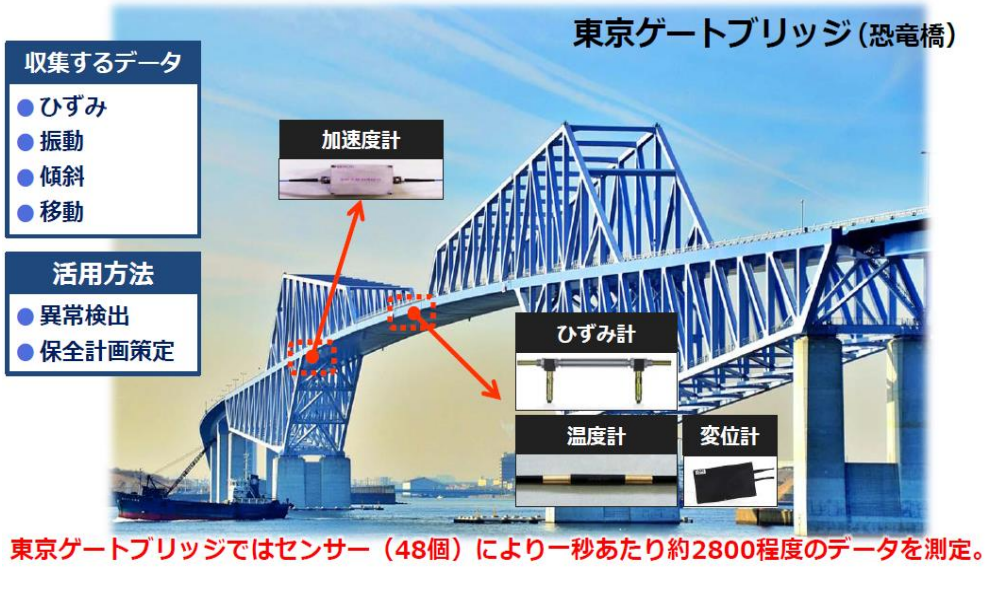


【出典】 JETRO「ニューヨークだより2017年2月」

■ 事例２）橋梁の保守・点検

・全国の橋梁は、高度成長期に作られたものが多く、老朽化。道路橋 約７０万の４０%がもうすぐ寿命。

・橋にセンサーを取り付け、道路橋のひずみ、振動、傾斜、移動などの異常や損傷を検知



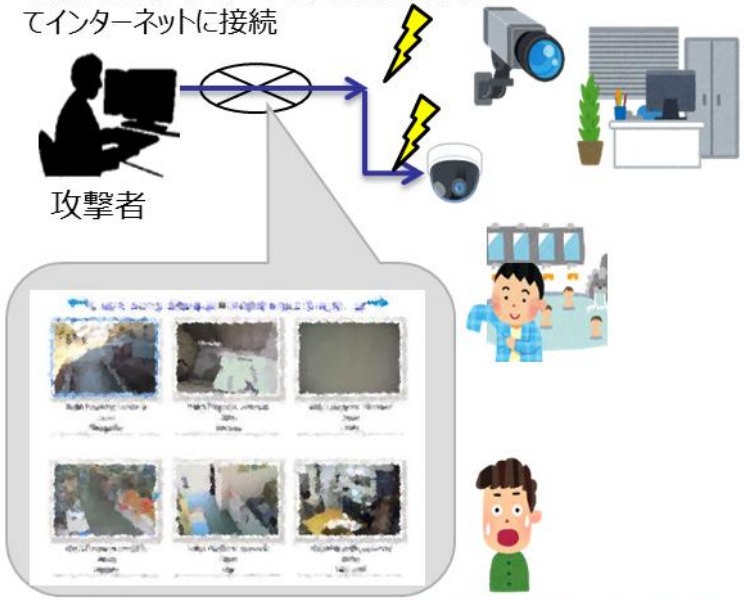
【出典】http://www.soumu.go.jp/main_content/000208995.pdf

人命や財産を脅かすリスクも！

IPA

監視カメラの映像がインターネット上に公開

利用者が気づかないまま、WiFi等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**。
（ID，パスワードなどの初期設定が必要）

自動車へのハッキングよる遠隔操作

携帯電話網経由で遠隔地からハッキング

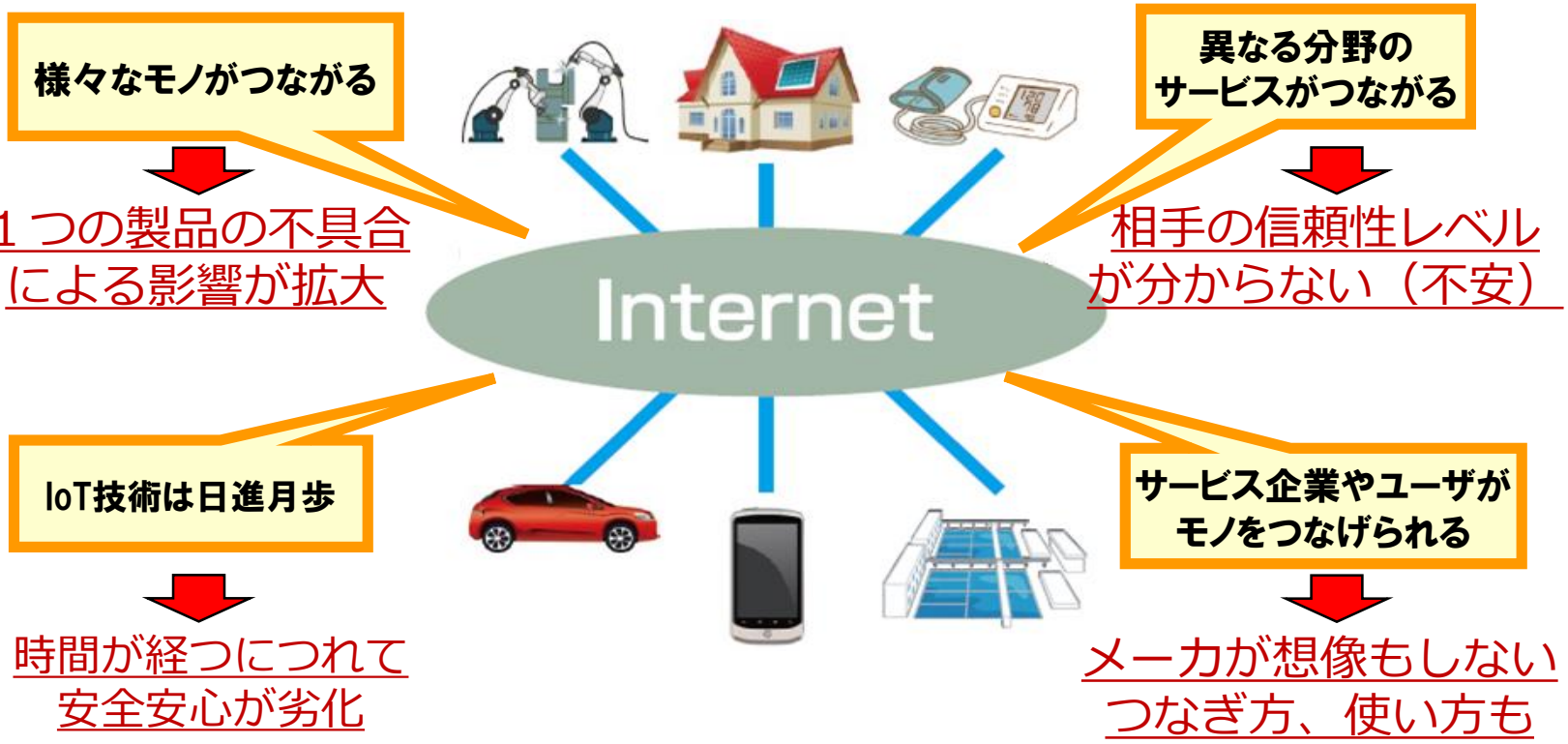
人命にも関わる事故が起こせることが証明され、
自動車会社は**140万台にも及ぶリコール**を実施。

【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

IoTのリスクを認識し、安全・安心への対策が急務！

つながる世界では様々な課題が存在

つながる世界では、製品供給者が想定しない、把握できない課題が発生



つながる世界の開発指針の概要

IoT機器・システムの開発者、保守者、経営者に最低限検討して頂きたい安全・安心に関する事項をライフサイクル視点で整理

◆つながる世界の開発指針の内容

目次
第１章 つながる世界と開発指針の目的
第２章 開発指針の対象
第３章 つながる世界のリスク想定
第４章 つながる世界の開発指針（１７個）
第５章 今後必要となる対策技術例

※指針は、ポイント、解説、対策例を記述

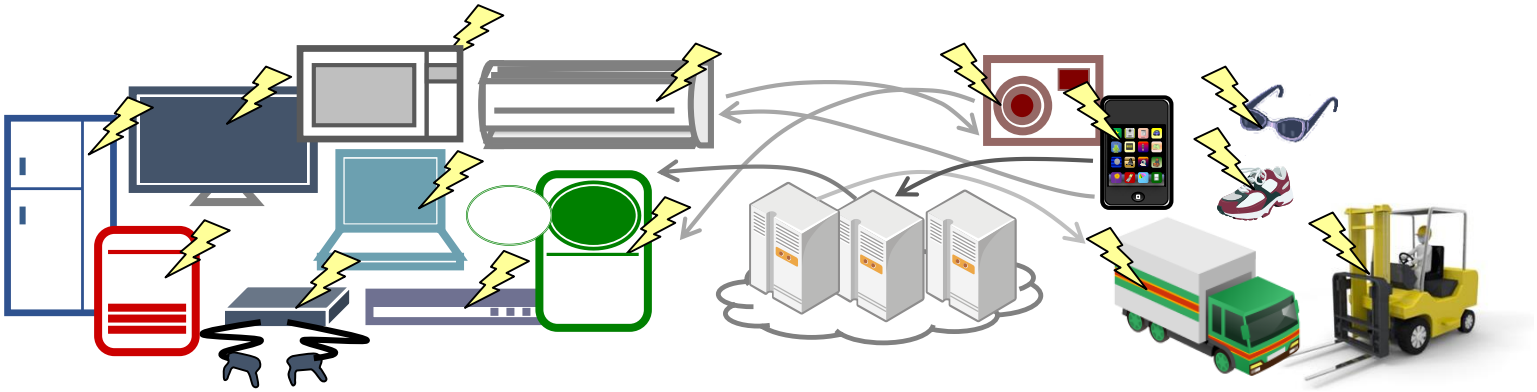
※開発指針を書籍化し、２０１６年5月１１日に発刊
http://www.ipa.go.jp/sec/reports/20160511_2.html

大項目		指針
方針	つながる世界の安全安心に企業として取り組む	指針1 安全安心の基本方針を策定する
		指針2 安全安心のための体制・人材を見直す
		指針3 内部不正やミスに備える
分析	つながる世界のリスクを認識する	指針4 守るべきものを特定する
		指針5 つながることによるリスクを想定する
		指針6 つながりで波及するリスクを想定する
		指針7 物理的なリスクを認識する
設計	守るべきものを守る設計を考える	指針8 個々でも全体でも守れる設計をする
		指針9 つながる相手に迷惑をかけない設計をする
		指針10 安全安心を実現する設計の整合性をとる
		指針11 不特定の相手とつなげられても安全安心を確保できる設計をする
		指針12 安全安心を実現する設計の検証・評価を行う
保守	市場に出た後も守る設計を考える	指針13 自身がどのような状態かを把握し、記録する機能を設ける
		指針14 時間が経っても安全安心を維持する機能を設ける
運用	関係者と一緒に守る	指針15 出荷後もIoTリスクを把握し、情報発信する
		指針16 出荷後の関係事業者に守ってもらいたいことを伝える
		指針17 つながることによるリスクを一般利用者に知ってもらう

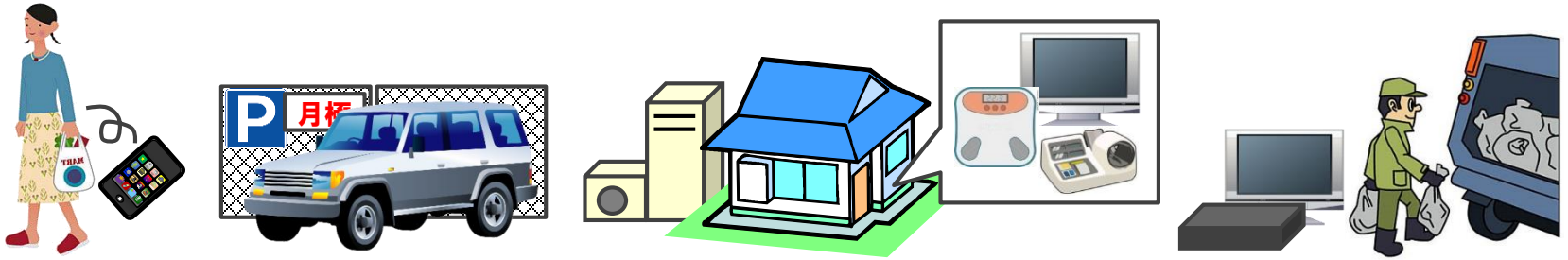
※IoTのネットワークに関する留意事項は、IoTセキュリティガイドラインを参照。
http://www.meti.go.jp/press/2016/07/20160705002/20160705002.html

つながる世界のリスクの特徴（１／２）

◆想定しないつながりが発生する



◆管理されていないモノもつながる



つながる世界のリスクの特徴（２／２）

◆ 身体や財産への危害にもつながる、危害がつながりにより波及する

◆ 問題が発生しても ユーザにはわかりにくい

開発指針の「方針」のポイント

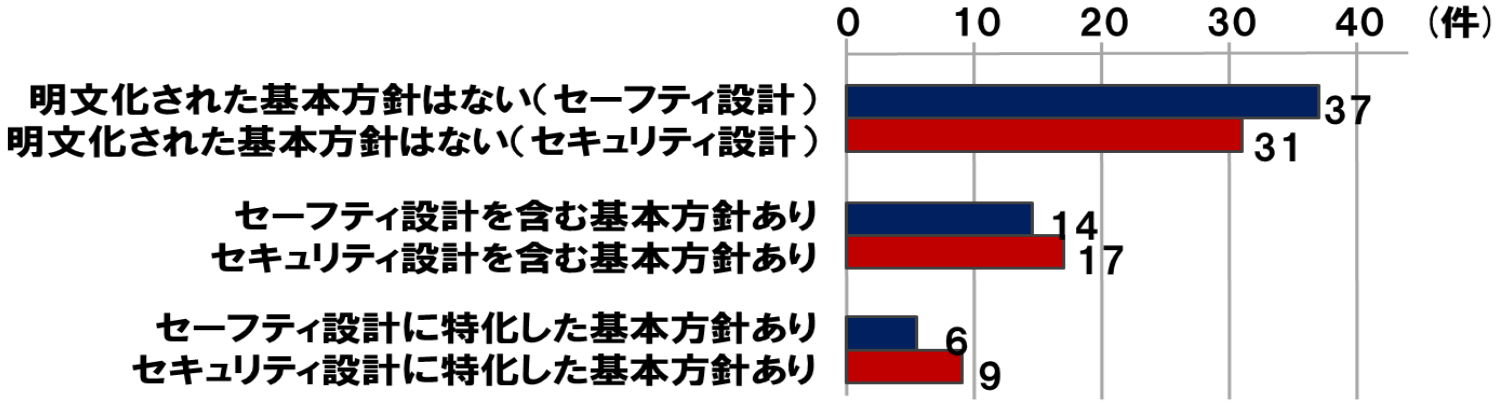
◆方針：つながる世界の安全安心に企業として取り組む

IoT時代の安全安心へのリスクは、経営問題となる可能性を認識し、企業の経営層に組織として取り組んでもらいたい事項をまとめた！

基本方針を策定する

体制・人材を見直す

内部不正やミスに備える

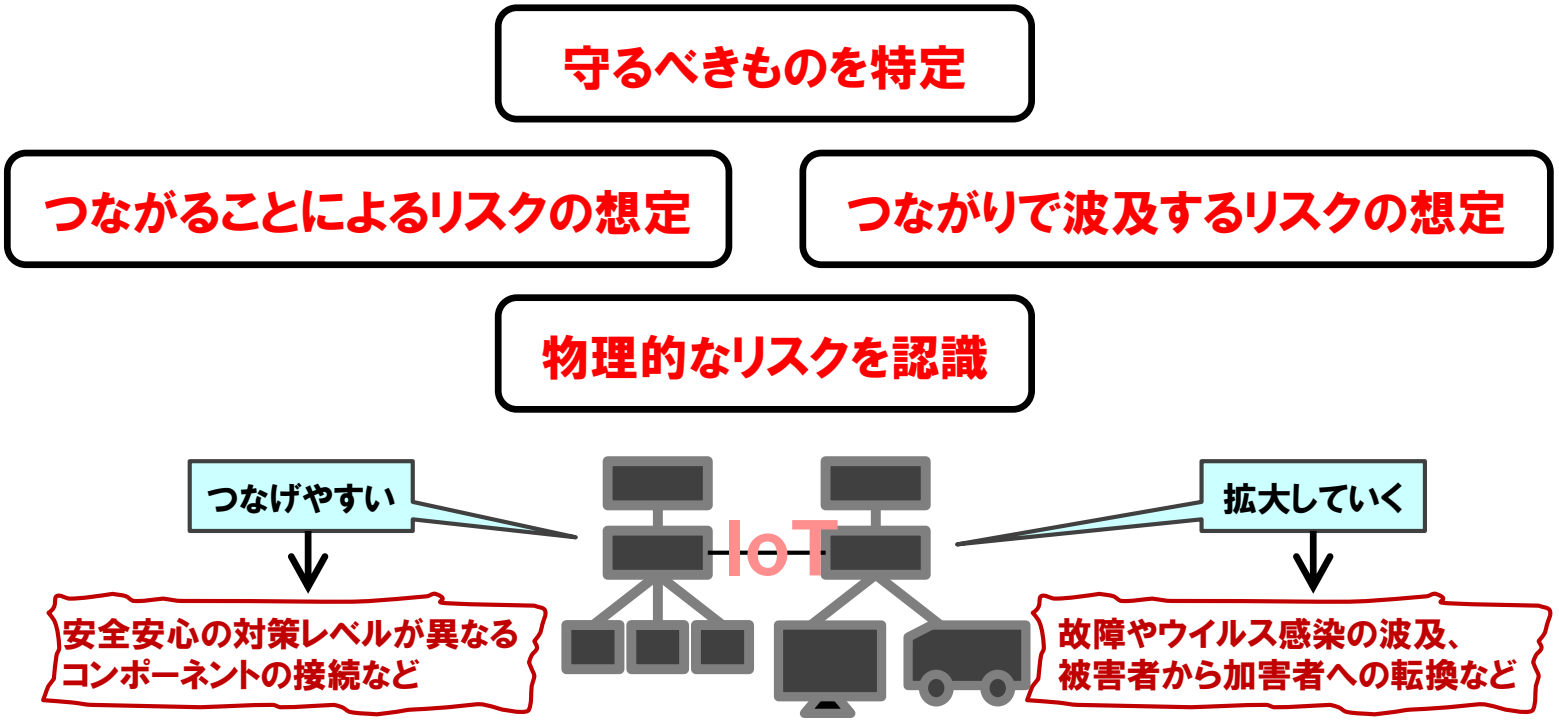


出典：IPA　セーフティ設計・セキュリティ設計に関する実態調査結果IPAアンケートより

開発指針の「分析」のポイント

◆分析：つながる世界のリスクを認識する

IoTの世界では、つながっていなかったモノがつながることで想定外の問題の発生や障害が波及するリスクなどの検討が必要！



開発指針の「設計」のポイント

◆設計：守るべきものを守る設計を考える

IoT機器にはリソースが小さいモノもあり、全体で守ることが重要。　また、障害の波及防止や接続相手の信用確認する仕組みも重要！

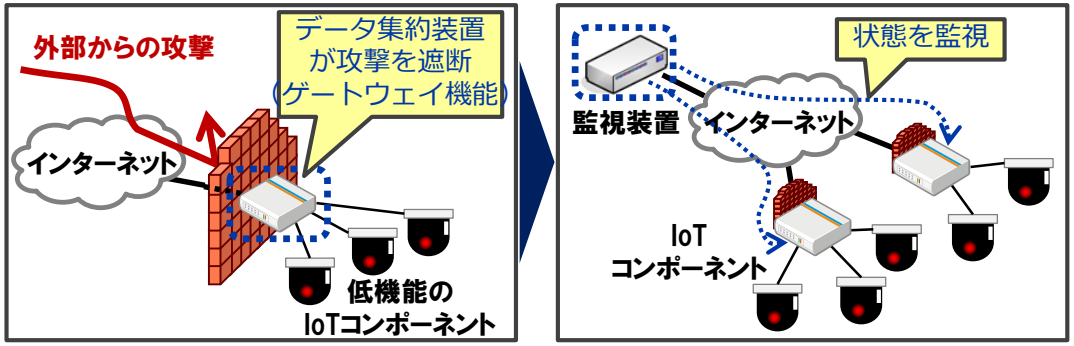
個々でも全体でも守る

つながる相手に迷惑を掛けない

不特定の相手とつなげられても安全安心を確保

安全安心の設計の整合を取る

安全安心の設計の検証・評価の実施



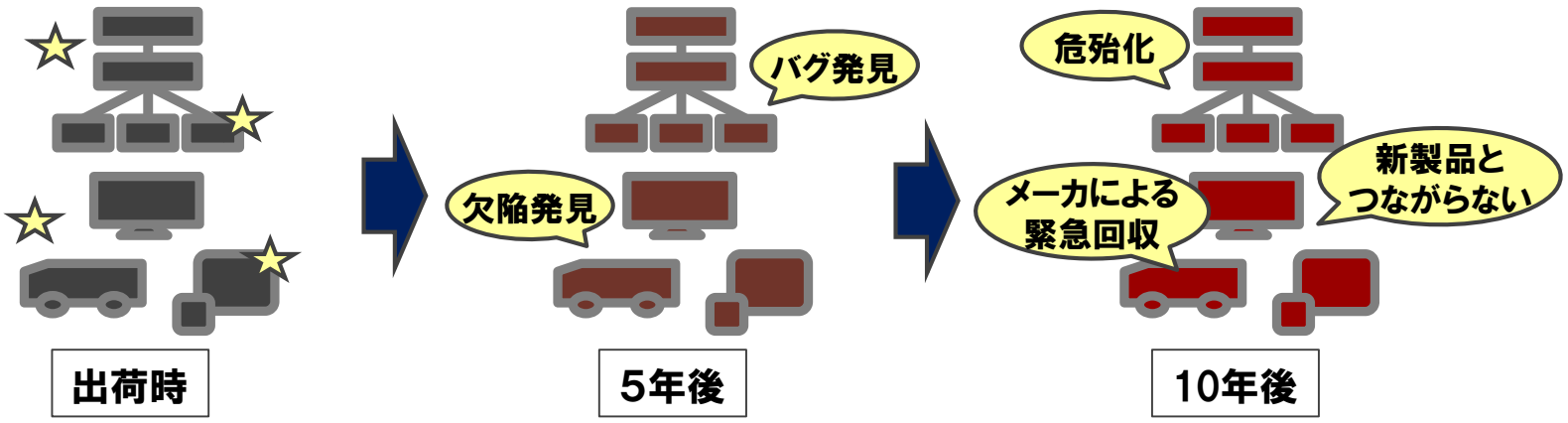
開発指針の「保守」のポイント

◆保守：市場に出た後も守る設計を考える

IoT機器には、10年以上も利用されるものも多く、故障やセキュリティ機能の劣化などの対策が必須。自分自身の状態を常に把握する機能や健全性を保つためにソフトウェアのアップデート機能は重要！

自身の状態を把握し記録する機能を設ける

時間が経っても安全安心を維持する機能を設ける



開発指針の「運用」のポイント

IPA

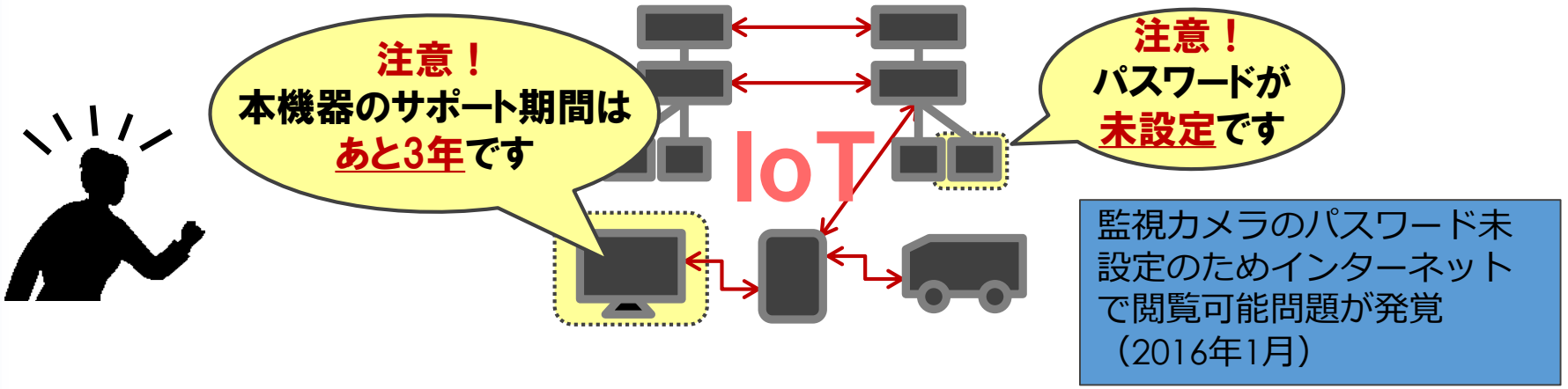
◆運用：関係者と一緒に守る

ログインパスワードの未設定問題やサポート期限切れ問題、廃棄時の個人情報・機密情報漏れ問題など運用に関わる懸念事項が多数あり、関係事業者との連携が重要！

出荷後もIoTリスクを把握し、情報発信する

関係事業者に守ってもらいたいこと伝える

一般利用者につながるリスクを伝える



「つながる世界の開発指針」の実践に向けた手引き

- **開発指針のうち技術面での対策を具体化し、高信頼化実現に必要な機能を策定**
- **2017年5月8日公開：以下のURLからpdf版のダウンロード、書籍の購入**
  http://www.ipa.go.jp/sec/reports/20170508.html

つながる世界の開発指針

2016年3月

「つながる世界の開発指針」の実践に向けた手引き

2017年5月

①設計段階から考慮して欲しい機能要件とIoT高信頼化機能の具体例を解説

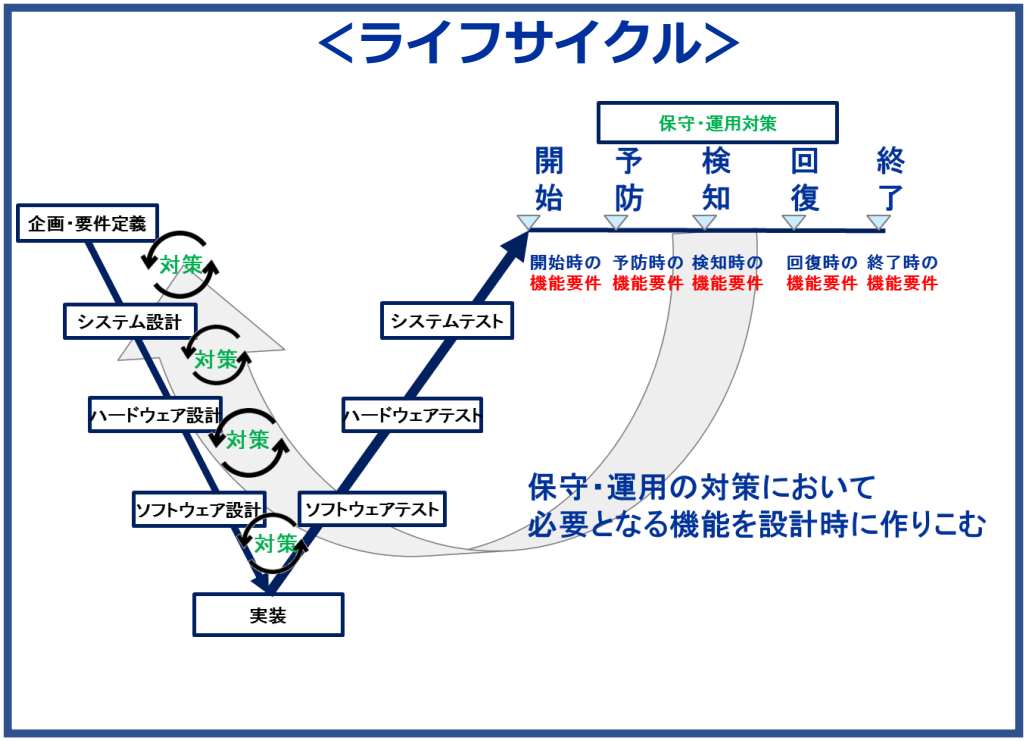
②IoT機器・システムやサービスのライフサイクルを意識し、クラウド・フォグ・エッジ等の機能配置も考慮

③IoTの分野間連携のユースケースによるリスクや脅威分析、対策として必要な機能や機能配置の具体例を提示

検討のスコープ（ライフサイクルと機能配置）

- IoT機器・システムのライフサイクルを考慮し、保守・運用で起こり得る様々な安全安心を阻害する事象に対応できることを目的に、IoTの利用開始から予防・検知・回復、終了の視点で、必要な機能を整理
- クラウド・フォグ・エッジ等の機能配置を考慮

→経済合理性や寿命を考慮し、全体として高信頼化を達成するための現実解を支援

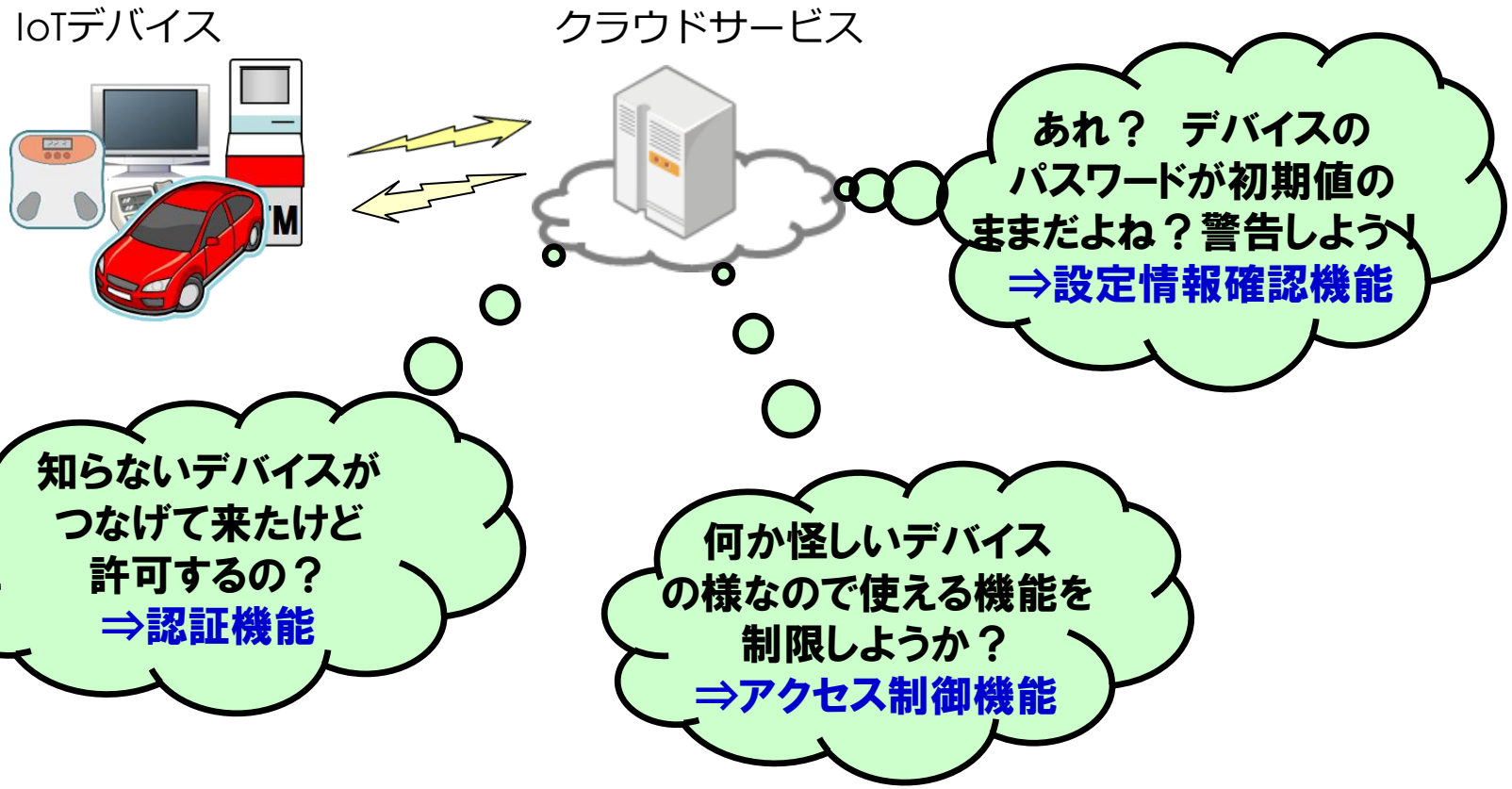


IoTの高信頼化の実現に向けた機能要件と機能

IoT高信頼化要件		IoT高信頼化のための１２の機能要件	実装に向けた２３の高信頼化機能
開始	導入時や利用開始時に安全安心が確認できる	1. 初期設定が適切に行われ、その確認ができる	初期設定機能、設定情報確認機能
		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	認証機能、アクセス制御機能
予防	稼働中の異常発生を未然に防止できる	3. 異常の予兆を把握できる	ログ収集機能、時刻同期機能、予兆機能、診断機能、ウイルス対策機能
		4. 守るべき機能・資産を保護できる	アクセス制御機能、ログ収集機能、時刻同期機能、ウイルス対策機能
		5. 異常発生に備えて事前に対処できる	リモートアップデート機能
検知	稼働中の異常発生を早期に検知できる	6. 異常発生を監視・通知できる	監視機能、状態可視化機能、
		7. 異常の原因を特定するためのログが取得できる	ログ収集機能、時刻同期機能
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	8. 構成の把握ができる	構成情報管理機能
		9. 異常が発生しても稼働の維持ができる	診断機能、隔離機能、縮退機能、冗長構成機能
		10. 異常から早期復旧ができる	リモートアップデート機能、停止機能、復旧機能、障害情報管理機能
終了	利用の終了やシステム・サービス終了後も安全安心が確保できる	11. 自律的な終了や一時的な利用禁止ができる	停止機能、操作保護機能、寿命管理機能
		12. データ消去ができる	消去機能

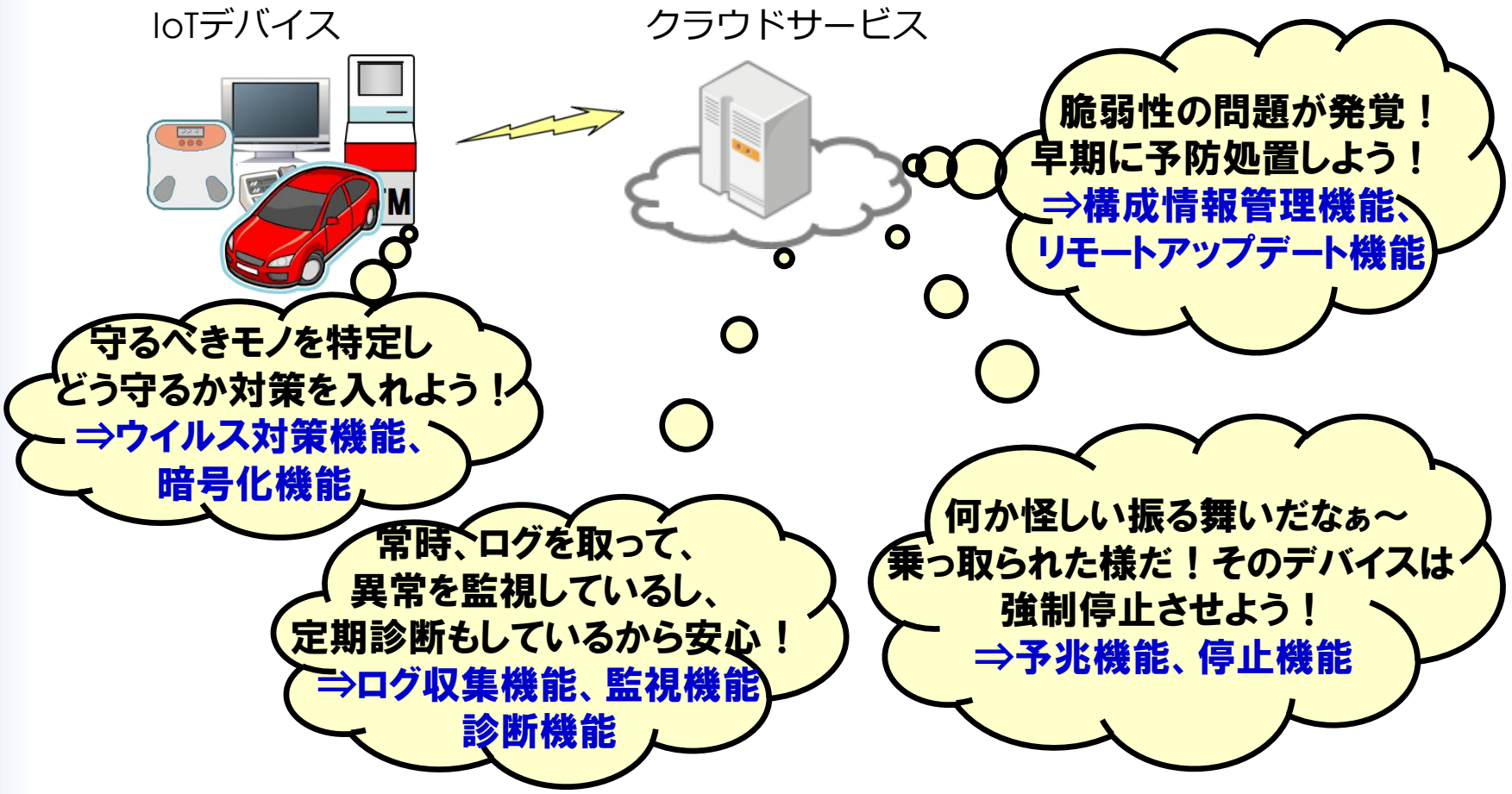
IoTの高信頼化対策は３つフェーズで考えよう！

（１）利用開始時に守る！（接続時の考慮）



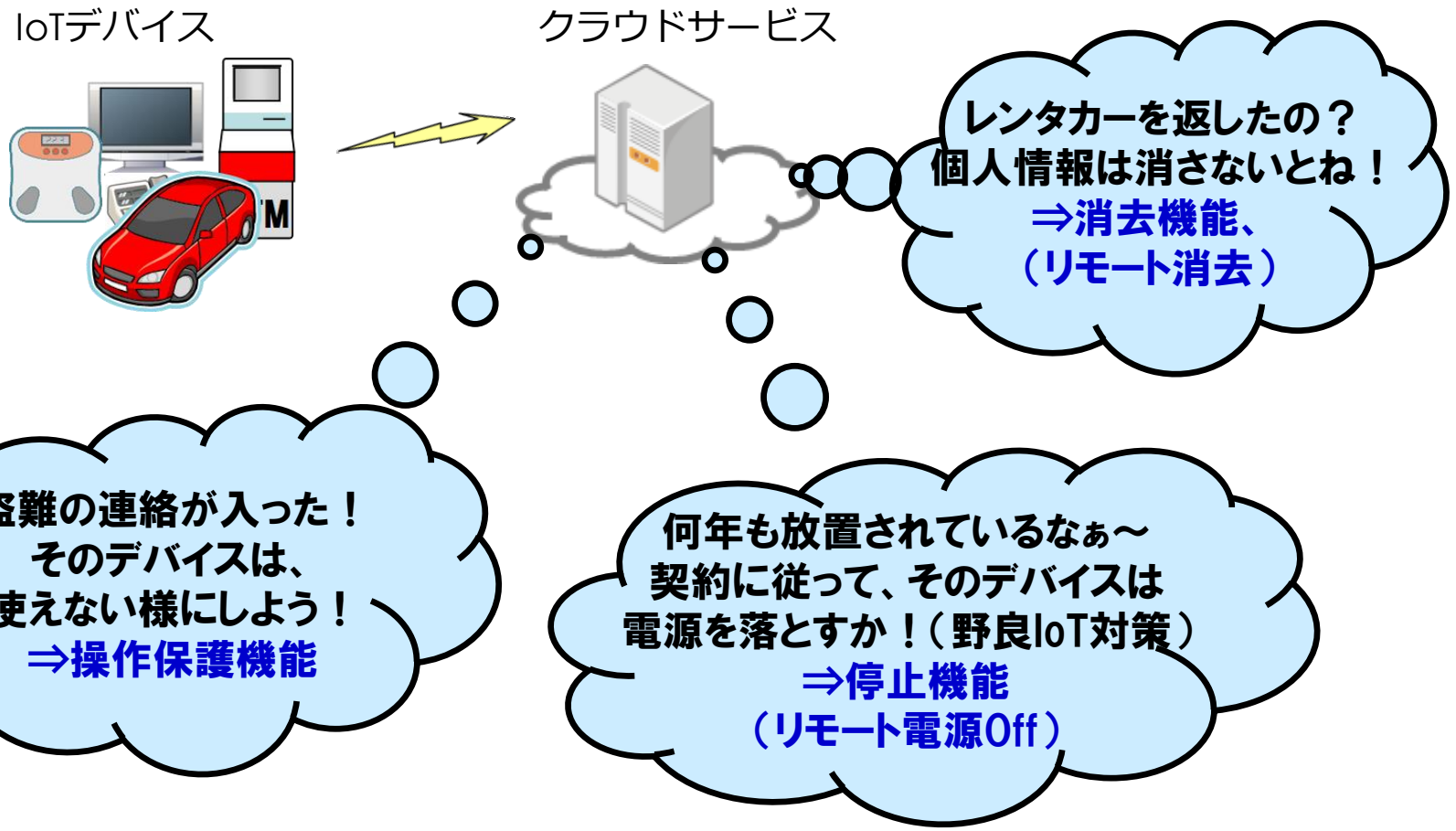
IoTの高信頼化対策は３つフェーズで考えよう！

（２）利用中に守る！（予防、検知、回復の考慮）



IoTの高信頼化対策は３つフェーズで考えよう！

（３）利用後も守る！（放置、リユース、廃棄時の考慮）



「つながる世界の開発指針」の展開

政府施策への展開

- IoT推進コンソーシアムのIoTセキュリティガイドラインへの展開（2016/7）
- ERABサイバーセキュリティガイドラインへの展開(2017/4)
- その他の政府レベルのガイドラインへの展開

国際標準化

- 国内外の産業界や海外の研究機関と連携した国際標準化
- JTC1/SC27,SC41に提案 (2018/5)

海外連携

- 米NISTと連携したIoTについての検討
- 独IESEと連携した実証実験

産業界への普及

- CCDS　4分野の分野別セキュリティガイドライン（2016/6）
- チェックリスト化、社内ルール化への支援(2017/3)
- その他の分野別ガイドラインの策定への支援

スコープ拡大

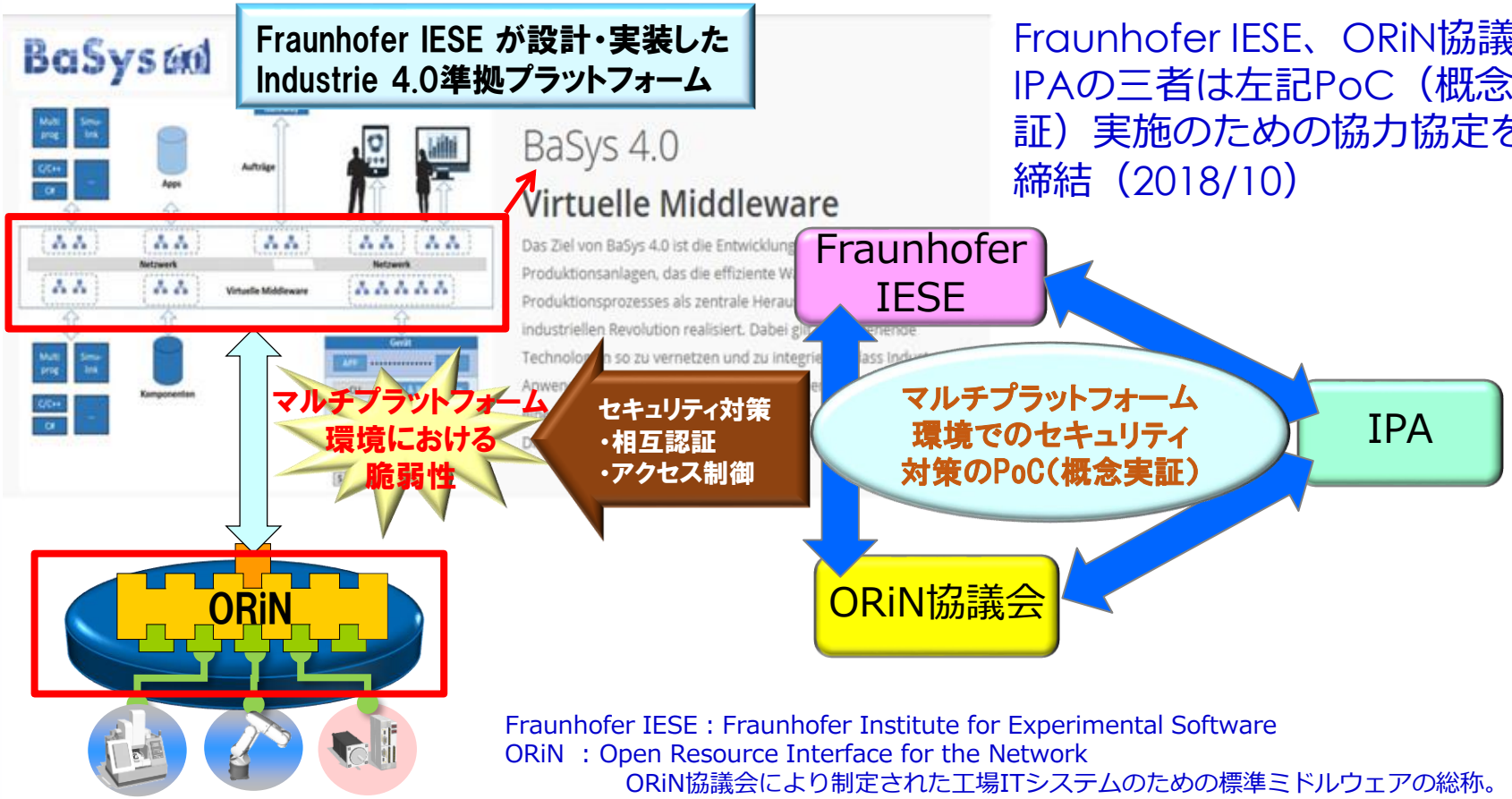
- IoT高信頼化に向けた機能要件と機能のまとめ(2017/5)
- 利用時品質のまとめ（HCD-netとの共創）(2017/3)
- **IoTの品質確保の視点（IVIA,CCDS等と共創）(2018/3)**
- データ品質の検討（データ流通推進協議会等と協調予定)

第2版：利用時の品質を製品開発の考慮点に追加(2017/6)

開発指針の海外連携による実証実験

◆海外連携による実証実験

Fraunhofer IESEとマルチプラットフォーム間のセキュリティ実証を計画中



Fraunhofer IESE、ORiN協議会、IPAの三者は左記PoC（概念実証）実施のための協力協定を締結（2018/10）

Fraunhofer IESE：Fraunhofer Institute for Experimental Software
ORiN ：Open Resource Interface for the Network
ORiN協議会により制定された工場ITシステムのための標準ミドルウェアの総称。
工場内の各機器に対して、メーカー、機種の違いを超えて統一的なアクセス手段と表現方法を提供。

開発指針の国際規格化に向けて

◆国際標準化

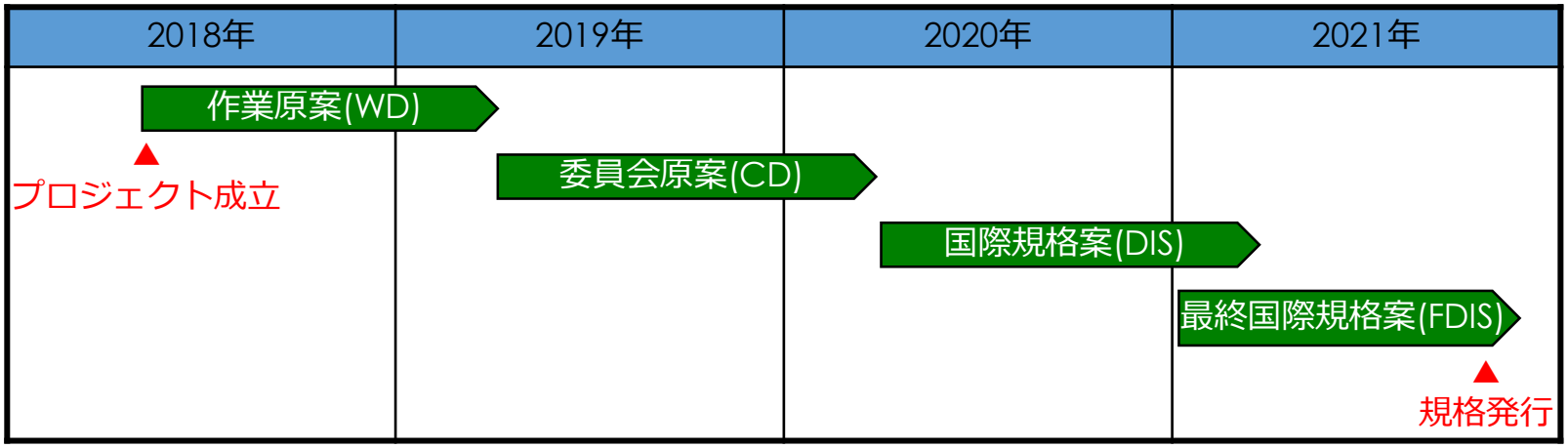
ISO/IEC JTC1/SC27、SC41に提案し、正式プロジェクトとして活動中

●SC27　IoTセキュリティの標準化

「つながる世界の開発指針」を取り込んだ「ＩｏＴセキュリティガイドライン」を基本としたセキュリティ確保の考え方を提案し、正式なプロジェクトとして発足。

●SC41 IoTの開発方法論の標準化

「安全なＩｏＴシステムのためのセキュリティに関する一般的枠組」等を基本としたセキュリティ確保のための方法論を提案し、正式なプロジェクトとして発足。



今回、ご紹介しました
「つながる世界の開発指針」は
これからIoT開発に着手する場合や
既に、開発済IoTに対するリスクの
ご確認にご活用いただけます。

ご清聴ありがとうございました。