IPA Better Life with IT

開発指針の実践によるオープンシステムディペンダビリティの実現

第５回 DEOS協会 オープン シンポジウム
2018年6月5日

独立行政法人情報処理推進機構（IPA)
技術本部ソフトウェア高信頼化センター（SEC)
調査役　宮原 真次

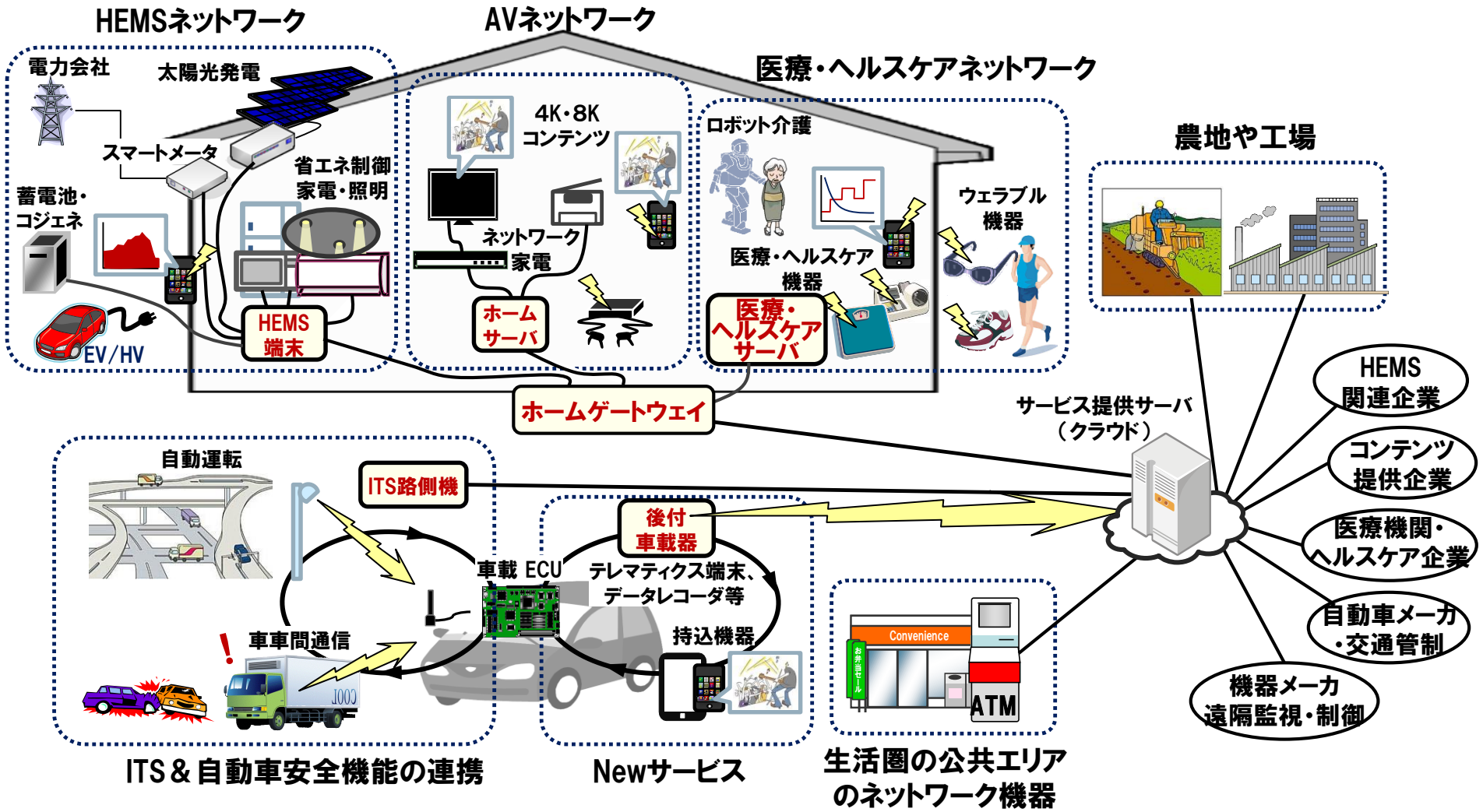
目 次

SEC
Software Reliability Enhancement Center

- IoT時代の安全安心の課題とリスク
- つながる世界の安全安心の実現に向けて
  - ～ つながる世界の開発指針の策定と関連施策 ～
- IoTにおけるオープンシステムディペンダビリティの実現
  - ～ 開発指針の実践によるOSD実現の考察 ～

IoT時代の安全安心の課題とリスク

IoT時代：様々なモノやサービスがつながる世界



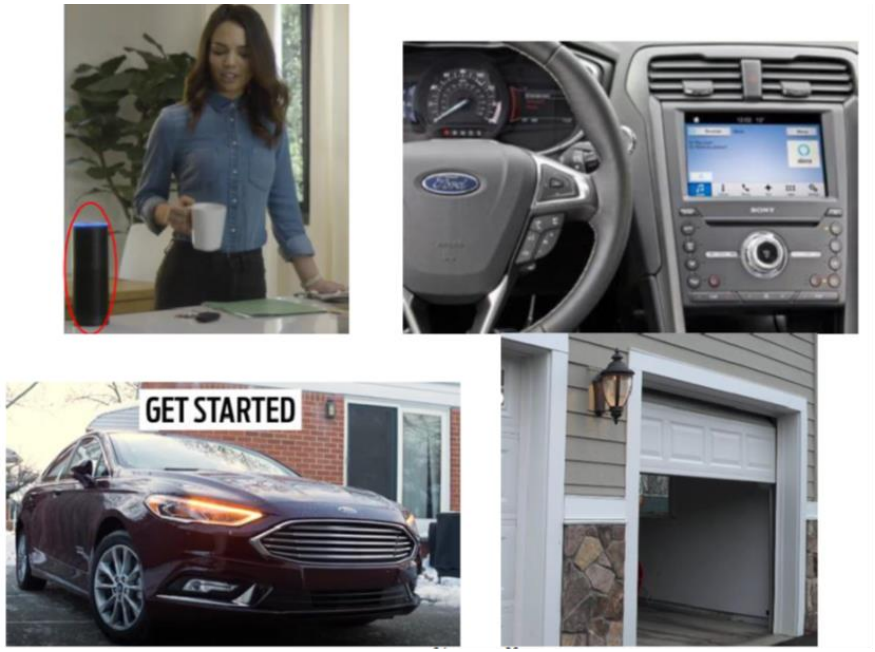
出典：一般社団法人重要生活機器連携セキュリティ協議会「セキュアライフ2020」中の図に加筆

IoT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

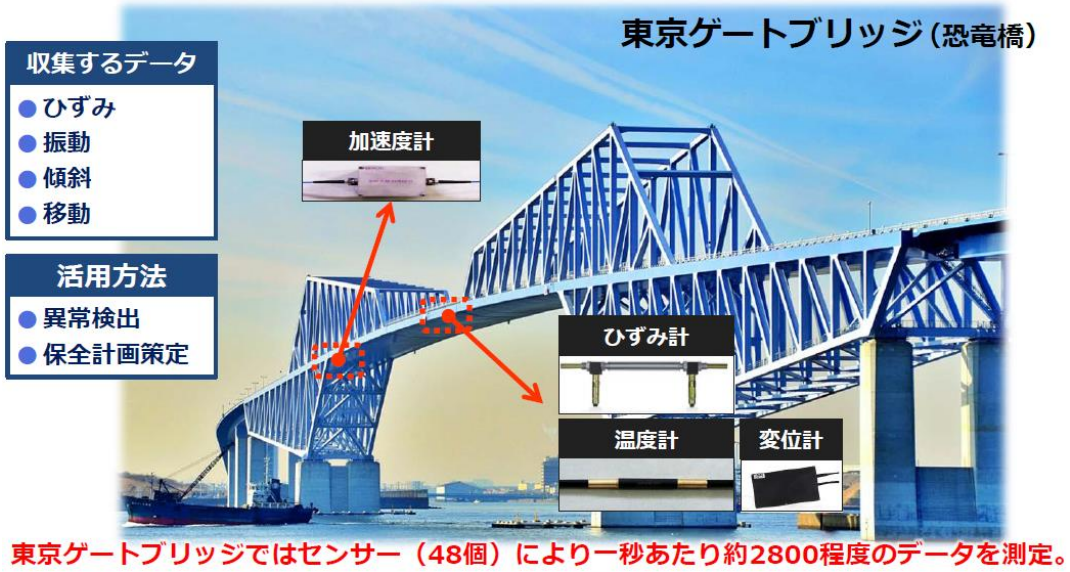


【出典】JETRO「ニューヨークだより2017年2月」

■ 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

つながる世界では様々な課題が存在

SEC
Software Reliability Enhancement Center

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

様々なモノがつながる

1つの製品の不具合による影響が拡大

異なる分野のサービスがつながる

相手の信頼性レベルが分からない（不安）

IoT技術は日進月歩

時間が経つにつれて安全安心が劣化

サービス企業やユーザがモノをつなげられる

メーカが想像もしないつなぎ方、使い方も

つながる世界では人命や財産を脅かすリスクも！

SEC Software Reliability Enhancement Center

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！

つながる世界の安全安心の実現に向けて

～　つながる世界の開発指針の策定と関連施策　～

つながる世界の安全安心の実現に向けた取組み

SEC Software Reliability Enhancement Center

1

2016年3月 公開

開発機能の具体化

検証評価の具体化

2

2017年5月 公開

「つながる世界の開発指針」の実践に向けた手引き【IoT高信頼化機能編】
高信頼化のためにIoT製品が満たすべき要件や具備すべき機能を解説

「つながる世界の開発指針」
IoT開発時に、その安全のために経営者や開発者が考慮すべき事項を取りまとめたもの

3

2018年3月 公開

「つながる世界の品質確保に向けた手引き」
IoT製品の品質を確保・維持するために、検証・評価・運用時に考慮すべき事項を取りまとめたもの

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

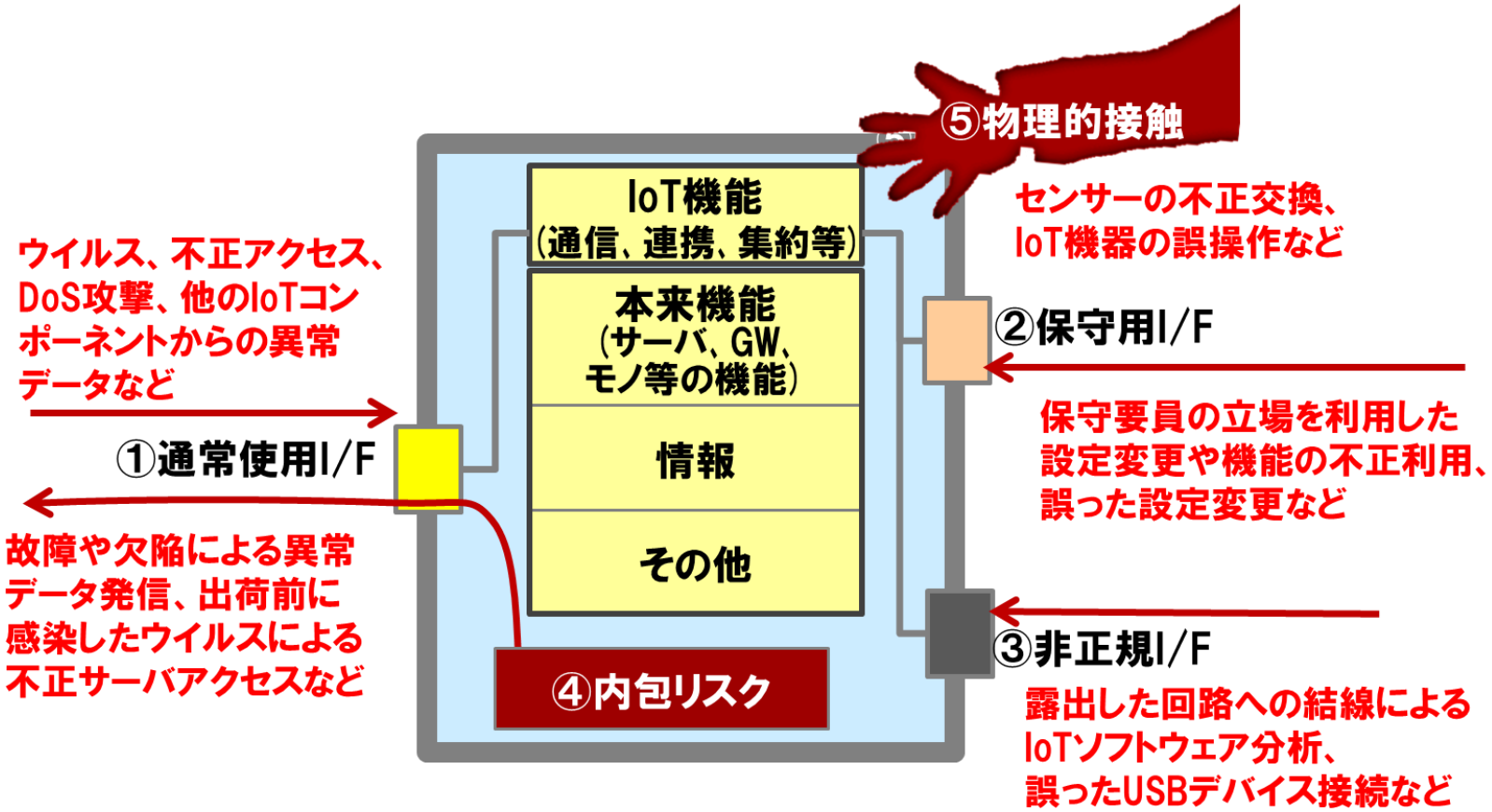
※開発指針を書籍化し、2016年5月11日に発刊
http://www.ipa.go.jp/sec/reports/20160511_2.html

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

つながる世界はリスクの想定が重要！

SEC Software Reliability Enhancement Center

■ 守るべきものを特定し、リスク箇所を整理（開発指針の捉え方）



IoTが使われる場面でリスク想定し、安全安心の対策を検討！

「つながる世界の開発指針」の実践に向けた手引き

SEC Software Reliability Enhancement Center

- **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にpdf版掲載**
  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

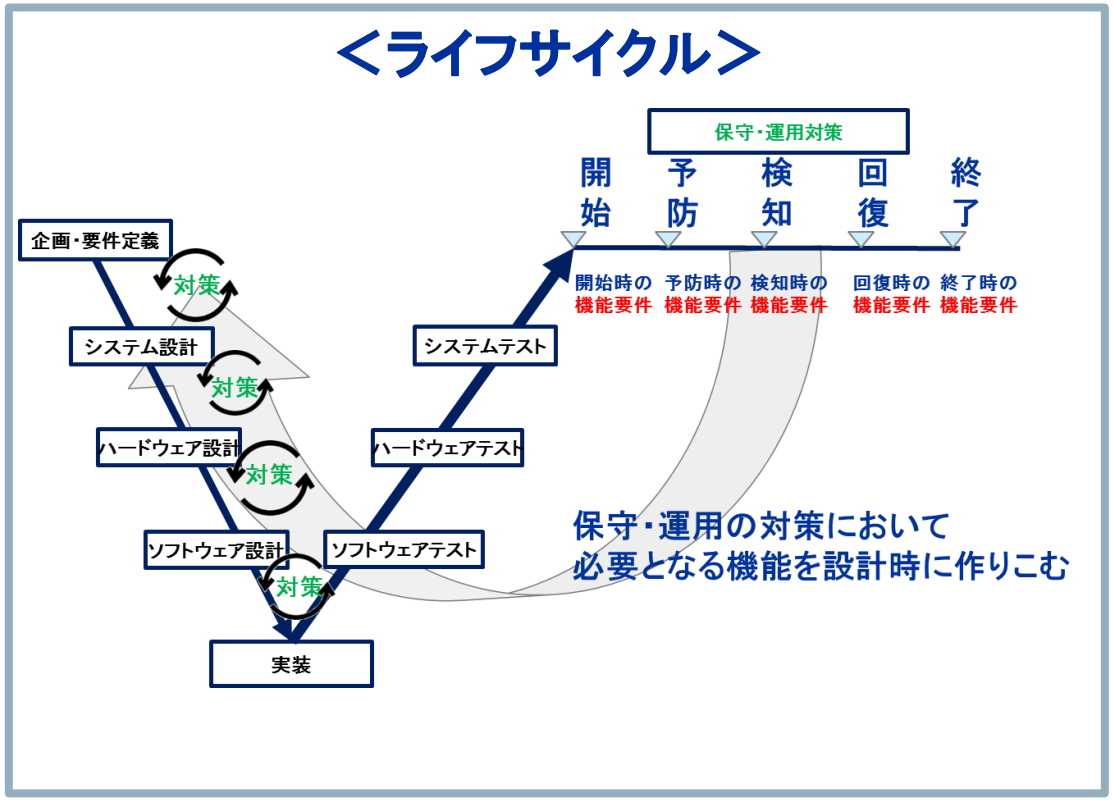
②IoT機器・システムやサービスのライフサイクルを意識し、クラウド・フォグ・エッジ等の機能配置も考慮

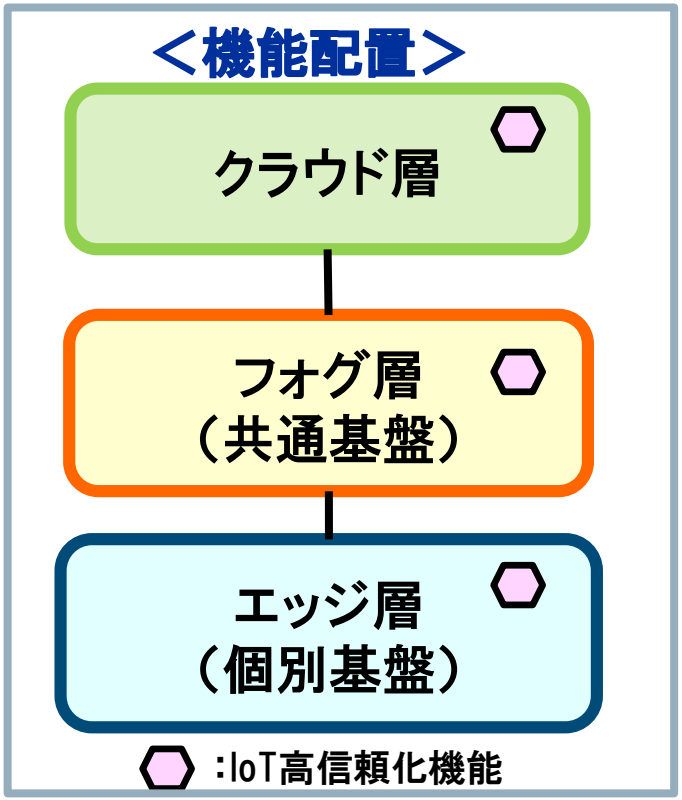
③IoTの分野間連携のユースケースによるリスクや脅威分析、対策として必要な機能や機能配置の具体例を提示

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

SEC Software Reliability Enhancement Center

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時代では品質確保が重要に！

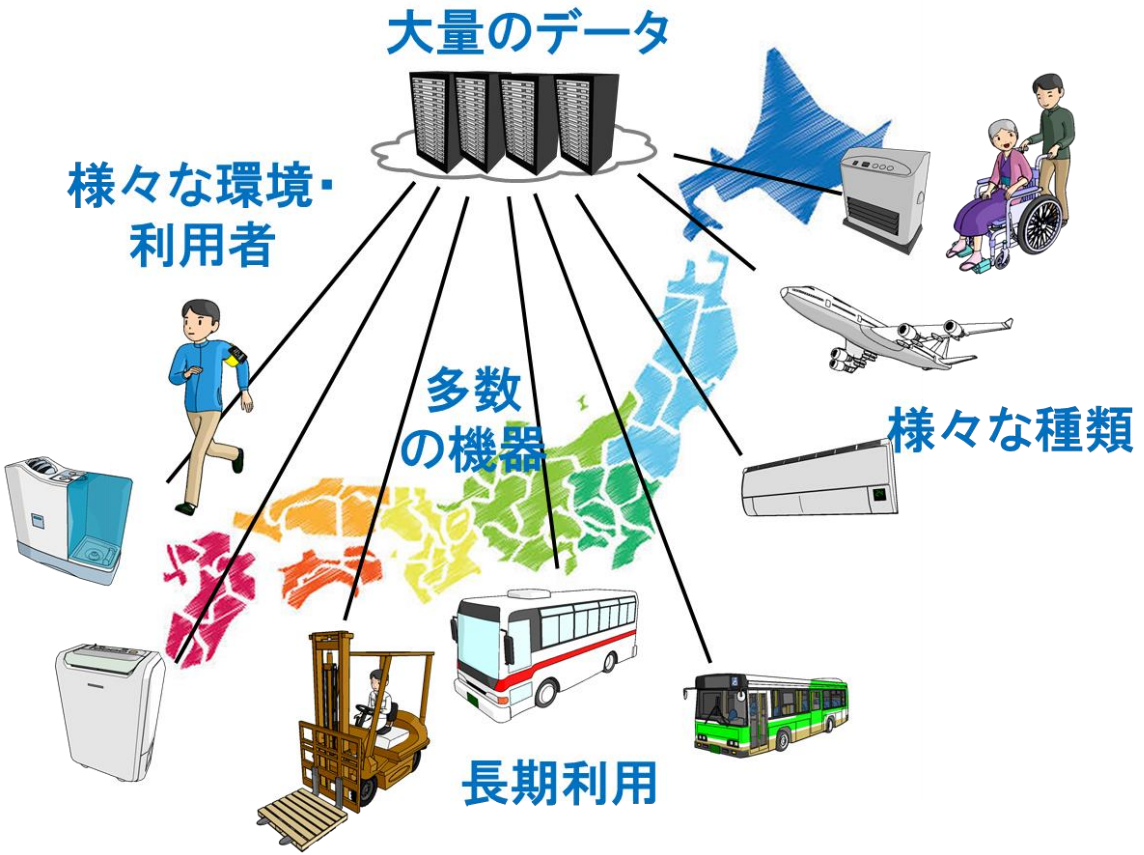
SEC
Software Reliability Enhancement Center

IoTの特徴

システムが日々変化！
接続される機器の種類や個数が膨大で、システムが日々刻々と変化

様々な環境で利用！
屋内/屋外、高地や寒冷地など様々な環境、幼児から高齢者まで幅広い層で利用

10年以上の長期利用！
自動車・家電製品・工場のシステムなど長期に利用



つながる世界の品質確保に向けた手引き（概要）

SEC Software Reliability Enhancement Center

- IoTの特徴を捉えて、IoTの品質確保で考慮すべき重要事項を13の視点として整理
- 開発者、保守者、品質保証者、運用者など品質に携わるすべての担当者が対象
- 2018年3月22日公開：以下のURLからpdf版ダウンロード
  https://www.ipa.go.jp/sec/reports/20180322.html

つながる世界の開発指針

2016年3月

2018年3月 公開

①IoTのライフサイクル全般で、品質を確保する活動を「V＆Vマネジメント」「妥当性確認」「検証」「運用マネジメント」「運用実施」の5つに整理し、品質確保のための考慮事項を解説

②IoTで実際に起こり得るIoTシステムの制御競合のケースを事例として、品質確保のための「13の視点」に基づき、適用検討事例を紹介

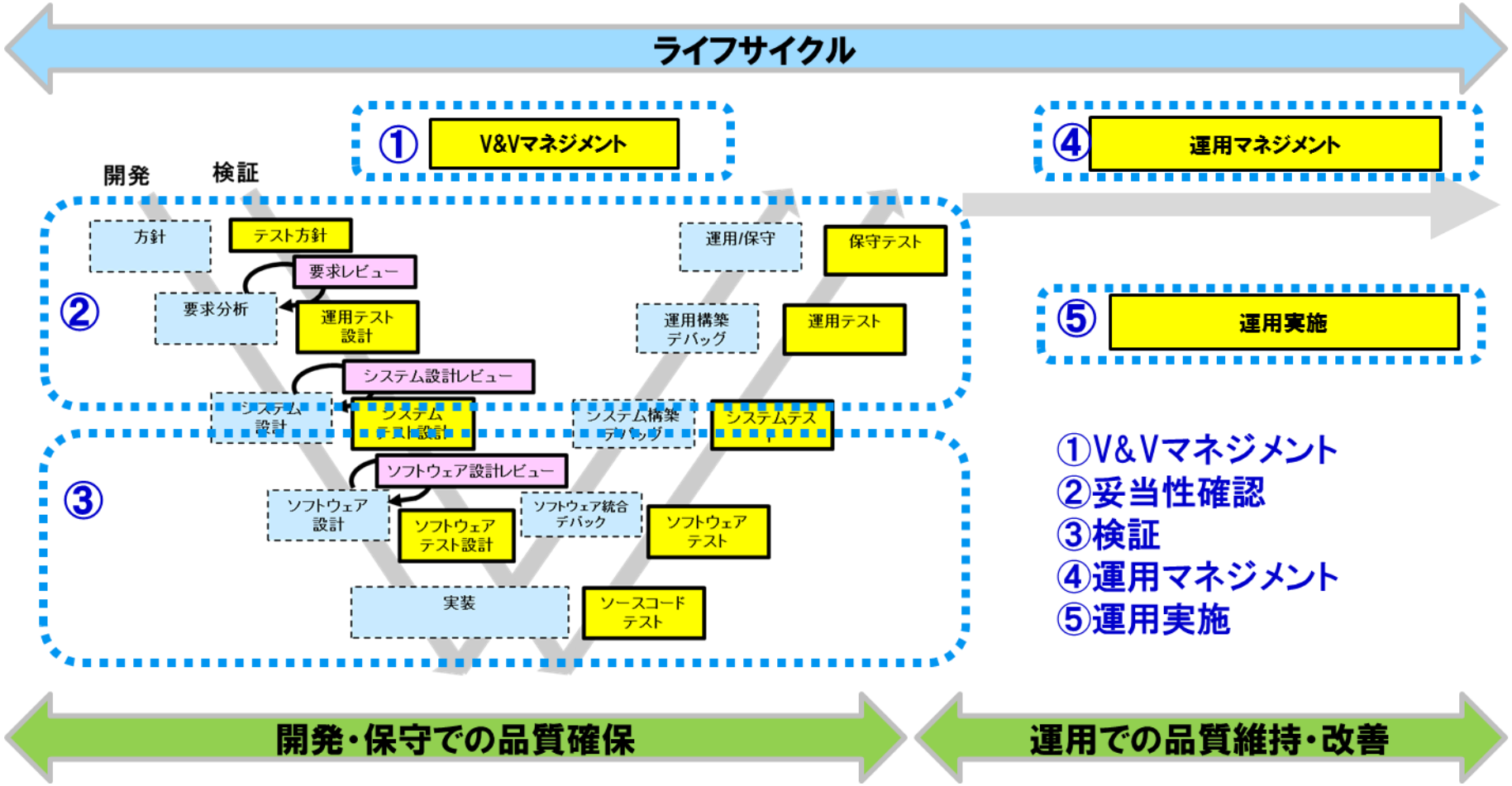
③開発・運用の現場で活用できる品質確保チェックリストを同時公開

※V&V：Verification and Validation（検証と評価）

IoTの品質確保、維持・改善のスコープ

SEC Software Reliability Enhancement Center

■ 品質を確保する5つの場面を想定し、そこで考慮すべき重点事項を整理



IoTの品質確保、維持・改善の13の視点

SEC Software Reliability Enhancement Center

IoTの開発・保守から運用までライフサイクルの品質に係わる重要事項を整理

	活動		品質の確保、維持・改善の視点
開発・保守	V&Vマネジメント	IoTの品質確保のための検証・評価計画立案	【視点1】IoTの社会的影響やリスクを想定する
	妥当性確認	利用者視点での要求の妥当性確認	【視点2】つながる機能の要求仕様が利用者を満足させるか確認する
			【視点3】実装した機能が利用者の要求を満たしているか評価する
	検証	IoTの特徴に着目したテスト設計	【視点4】多種多様なつながり方での動作と性能に着目する
			【視点5】多種多様な利用環境や使い方に着目する
			【視点6】障害や故障、セキュリティ異常の検知と回復に着目する
			【視点7】長期安定稼働の維持に着目する
			【視点8】大規模・大量データのテスト環境構築とテスト効率化を検討する
			【視点9】テストのし易さと実施可能性を検討する
		IoTの効率的なテスト実施	【視点10】テストを効率的に実施し、エビデンスを残す
運用	運用マネジメント	IoTの品質を維持・改善するための運用計画立案	【視点11】運用中の環境変化による影響やリスクを想定する
	運用実施	長期利用での品質維持と改善	【視点12】運用中の環境変化を捉え、品質が維持されているか確認する
			【視点13】ソフトウェアの更新時はつながる相手への影響を確認する

IoTにおけるオープンシステム
ディペンダビリティの実現

～　開発指針の実践によるOSD実現の考察　～

オープンシステムディペンダビリティの4つの視点

SEC Software Reliability Enhancement Center

OSD:「システムの目的，目標，環境及び性能の変更に対応し，不断に説明責任を遂行することによって，期待されるサービスを求められた時に求められたように提供する能力」のことである。

合意形成プロセスビュー：

システム，システムの目的，目標，環境，性能，ライフサイクル，及びこれらの変化に関する共通理解と明示的合意を確立し，維持する

障害対応プロセスビュー：

障害に際してもサービス中断と損害を最小にとどめ，その状況のもとで最も適切なやり方で，可能な限りサービス提供を続ける

説明責任遂行プロセスビュー：

システムに関する合意事項の不履行がステークホルダや一般社会に及ぼす影響を同定し，合意事項の遂行を改善して，システムに関する確信と信用を保ち，潜在的な被害に対する補償を確実にする

変化対応プロセスビュー：

要求，環境，目標及び目的が変化しても，システムの「目的にかなった（fit-for-purpose）」状態を維持する

出典：http://deos.or.jp/link/obj/pdf/DEOS-TR-20180125.pdf

IoT開発におけるOSDの実現

SEC Software Reliability Enhancement Center

つながる世界の開発指針シリーズ

×

オープンシステムディペンダビリティ

- 合意形成プロセスビュー
- 障害対応プロセスビュー
- 説明責任遂行プロセスビュー
- 変化対応プロセスビュー

現場への適用

IoTの開発において、開発指針をプロセスへ展開する時や機能の実装検討、検証・評価の検討に関して、OSDの4つの視点でレビューすることで、抜け漏れ防止が期待できる。

※つながる世界の開発指針シリーズは、最低限検討が必要な重点事項が記述されており、現場への適用展開には、OSDの視点は補完的な意味でも有効と考えられる。

事例1：開発指針の展開（OSD視点によるレビュー）

SEC Software Reliability Enhancement Center

つながる世界の開発指針

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
設計	守るべきも守る設計をる	
保守	市場に出た守る設計をる	
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

オープンシステムディペンダビリティの4つの視点

合意形成	説明責任遂行	障害対応	変化対応
・基本方針が社内や関係者に共通理解が得られ、明示的に合意できるものになっているか。	・基本方針をステークホルダに周知し、そのフィードバックが得られる仕組みを考慮しているか。	・基本方針に障害を想定した対応やインシデント対応の体制が考慮されているか。	・基本方針にIoTシステムの環境や性能の変化の把握と対応方針が明確化されているか。

事例2：IoT高信頼化機能の展開（OSD視点によるレビュー）

SEC Software Reliability Enhancement Center

開発指針の実践に向けた手引き[IoT高信頼化機能編]

IoT高信頼化要件		IoT高信頼化のための12の機能要件
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
		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
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
		4. 守るべき機能・資産を保護できる
		5. 異常発生に備えて事前に対処できる
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
		7. 異常の原因を特定するためのログが取得できる
回復	常が発生 の維持 旧ができ	8. 構成の把握ができる
終了	利用の終了 ム・サービ も安全安心 きる	

オープンシステムディペンダビリティの4つの視点

合意形成	説明責任遂行	障害対応	変化対応
・異常発生時の初期対応や原因究明に向けた関係者間での役割などの合意形成ができているか。	・異常発生のメカニズムの解明と説明責任が果たせる情報収集の機能が考慮されているか。	・異常の検知が出来ないものを同定し、減災のための総括的な対応が考慮されているか。	・IoTの環境や利用者の変化が把握でき、機能や性能への影響を確認する手段が考慮されているか。

事例3：品質確保に向けた手引きの展開（OSD視点によるレビュー）

SEC Software Reliability Enhancement Center

品質確保に向けた手引き

	活動	品質の確保、維持・改善の視点
開発・保守	V&Vマネジメント [検証・評価計画]	【視点1】 IoTの社会的影響やリスクを想定する
	妥当性確認 [要求の妥当性確認]	【視点2】 つながる機能の要求仕様が利用者を満足させるか確認する
		【視点3】 実装した機能が利用者の要求を満たしているか評価する
		【視点4】 多種多様なつながり方での動作と性能に着目する
		【視点5】 多種多様な利用環境や使い方に着目する
	検証 [テスト計画、テスト実施]	
運用	運用マネジメン [運用計画]	
	運用実施 [品質維持]	
		【視点13】 ソフトウェアの更新時はつながる相手への影響を確認する

オープンシステムディペンダビリティの4つの視点

合意形成	説明責任遂行	障害対応	変化対応
・要求仕様は様々なステークホルダの要求を考慮しているか。また、合意形成の手段が考慮されているか。	・要求仕様の妥当性確認の結果が様々なステークホルダにフィードバックされているか。	・サービス継続の視点で要求仕様に障害の回避/回復/復旧手段が考慮されているか。	・サービスイン後の法規制の変化や脆弱性対策の変化など、運用で必要な情報収集が考慮されているか。

世界をリードするIoTの実現を目指して

SEC
Software Reliability Enhancement Center

IoT時代の安全安心な世界の実現

協調した活動

IPA：つながる世界の開発指針の普及

DEOS協会：OSD(IEC62853)の普及

- 合意形成プロセスビュー
- 障害対応プロセスビュー
- 説明責任遂行プロセスビュー
- 変化対応プロセスビュー

最後に、「つながる世界の開発指針」の今後の展開

SEC Software Reliability Enhancement Center

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の品質確保の検討（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年6月)

ご清聴ありがとうございました。