IPA Better Life with IT

つながる世界の安全安心の確保に向けて
～IoT高信頼化機能とディペンダビリティ～

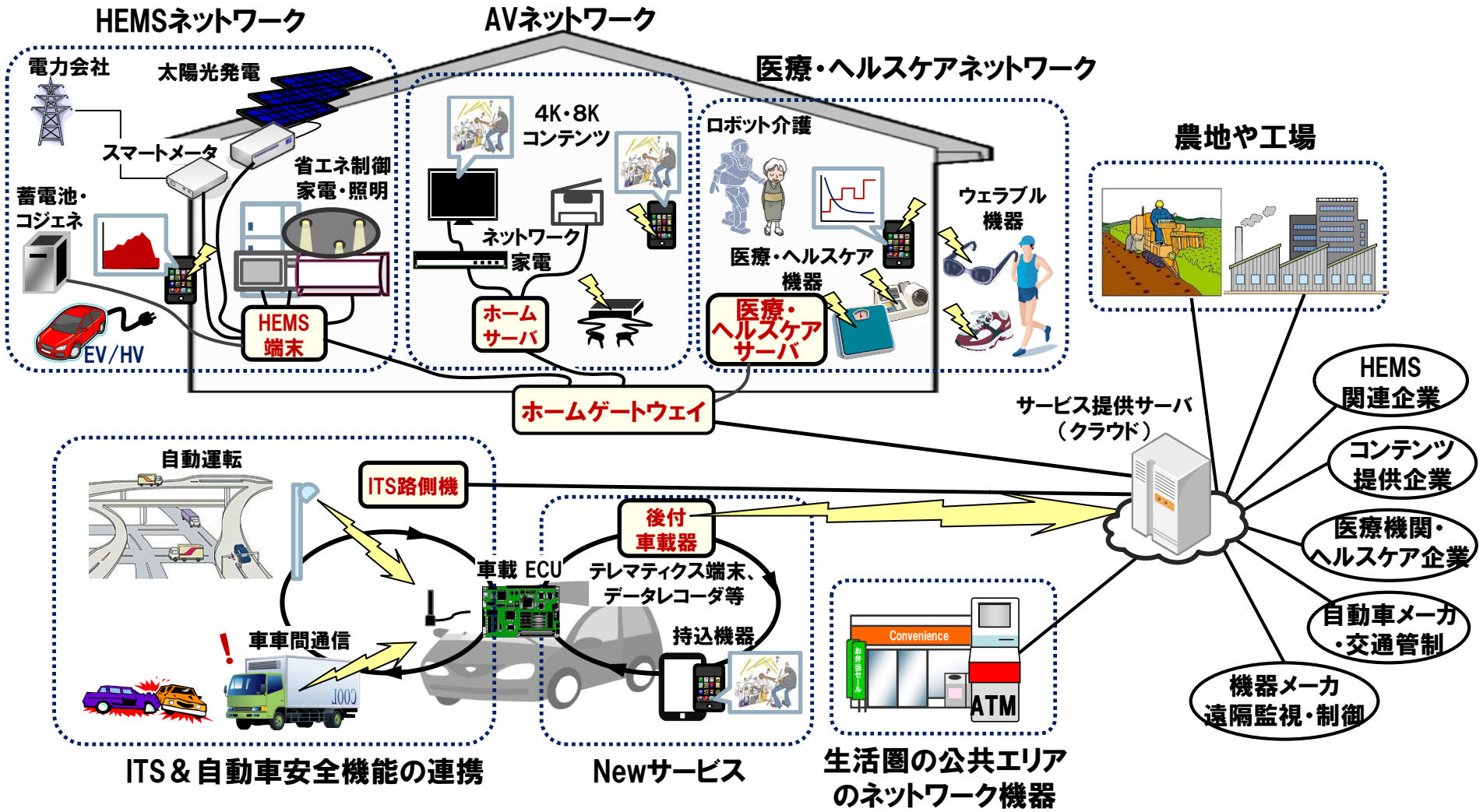
第二回 DEOS協会 OSD シンポジウム
2017年11月21日

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

- IoT/CPSのイメージと適用事例
- つながる世界の課題認識とリスク事例
- つながる世界の安全安心に向けたSECの取組み
- つながる世界とディペンダビリティ
- つながる世界の開発指針の今後の展開

IoT時代：様々なモノやサービスがつながる世界

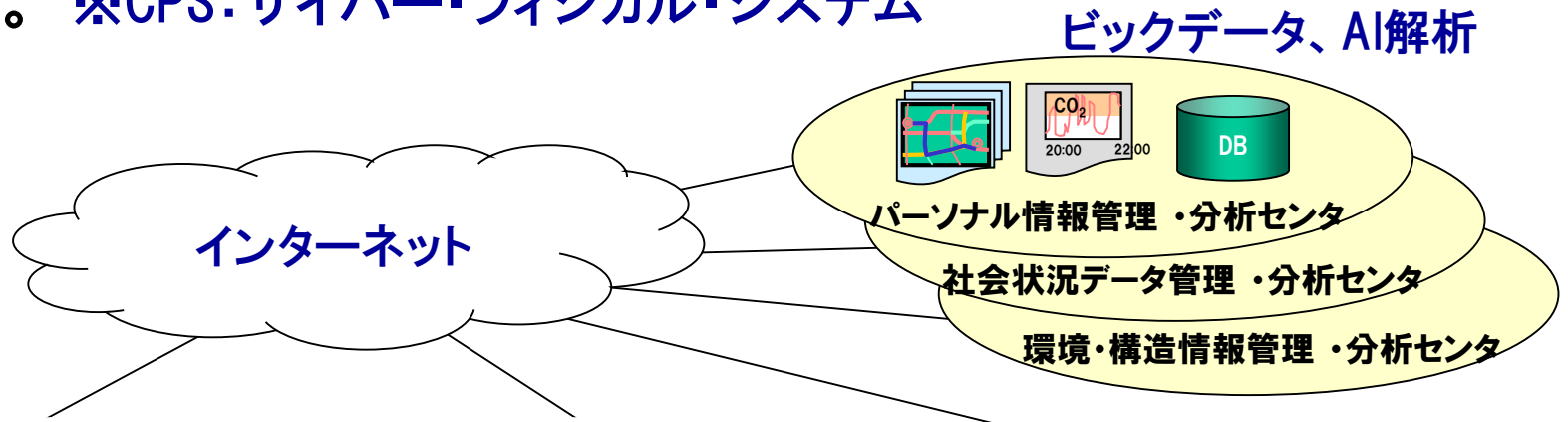


出典：一般社団法人重要生活機器連携セキュリティ協議会「セキュアライフ2020」中の図に加筆

CPS社会：大量のセンサーデータを分析・活用する世界

SEC Software Reliability Enhancement Center

個人から地球環境まで、あらゆるところにセンシングデバイスが遍在する社会が到来。 ※CPS：サイバー・フィジカル・システム



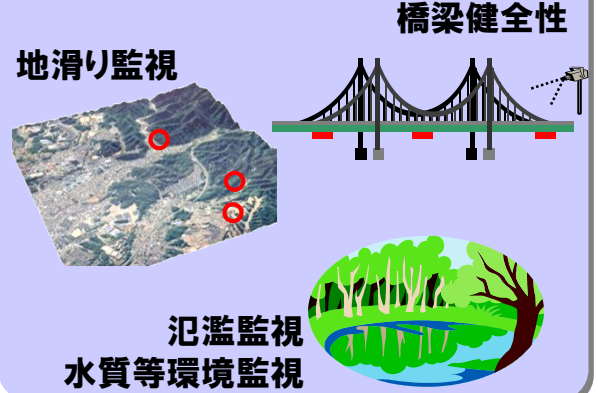
パーソナル情報センシング

個人の健康状態や屋内外の環境因子をセンシングし、ヘルスケア情報を提供

社会状況センシング

社会状況をセンシングし、渋滞回避等の次のアクションのための意思決定支援情報を提供

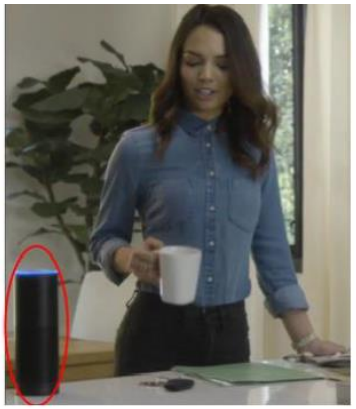
環境・構造情報センシング



環境・構造情報をセンシングし、可視化情報や将来予測等のアセスメント情報を提供

分野間連携事例）スマートハウスとスマートカー連携

- Ford社の車載情報システム「SYNC 3」と宅内にあるAmazon社の「Amazon Echo」が連携し、宅内から車内、車内から宅内の操作が可能になる
- 例）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」
https://www.jetro.go.jp/ext_images/_Reports/02/21ff0f61ce84fd8e/rpNy-201702.pdf

保守効率化事例）JR東日本「スマートメンテナンス」

SEC Software Reliability Enhancement Center

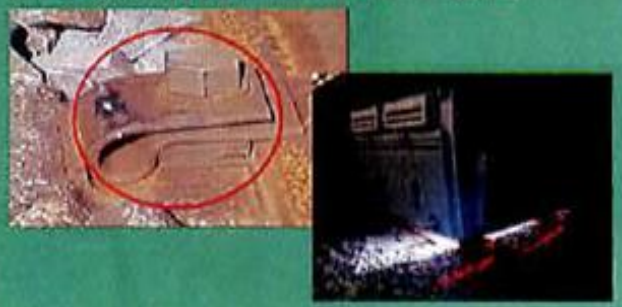
センサ・ビックデータを活用した保守コストの大幅削減
～　時間計画保全から状況監視保全へ　～

○さらなる安全・安定輸送の確保をめざし、ＩＣＴを活用した業務革新を推進。その一環として、高頻度に線路状態の変化を把握する「線路設備モニタリング装置」 を開発中。

○２０１３年５月より、京浜東北線Ｅ２３３系営業用車両１編成に「線路設備モニタリング装置」を搭載し、機器の性能及び取得データに関する検証を開始。

■「線路設備モニタリング装置」の主な機能

（１）軌道材料モニタリング装置



※ カメラによりレール締結装置などを撮影。画像解析により、レール締結装置の状態などを抽出。

（２）軌道変位検測装置

※加速度計とレーザーセンサーにより、線路状態の変化を測定。

「スマートメンテナンス」機能搭載を予定している
JR山手線の新型車両「E235系」

出典：JR東日本WEB、ITproニュース2014.8.26記事

つながる世界の課題認識とリスク事例

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

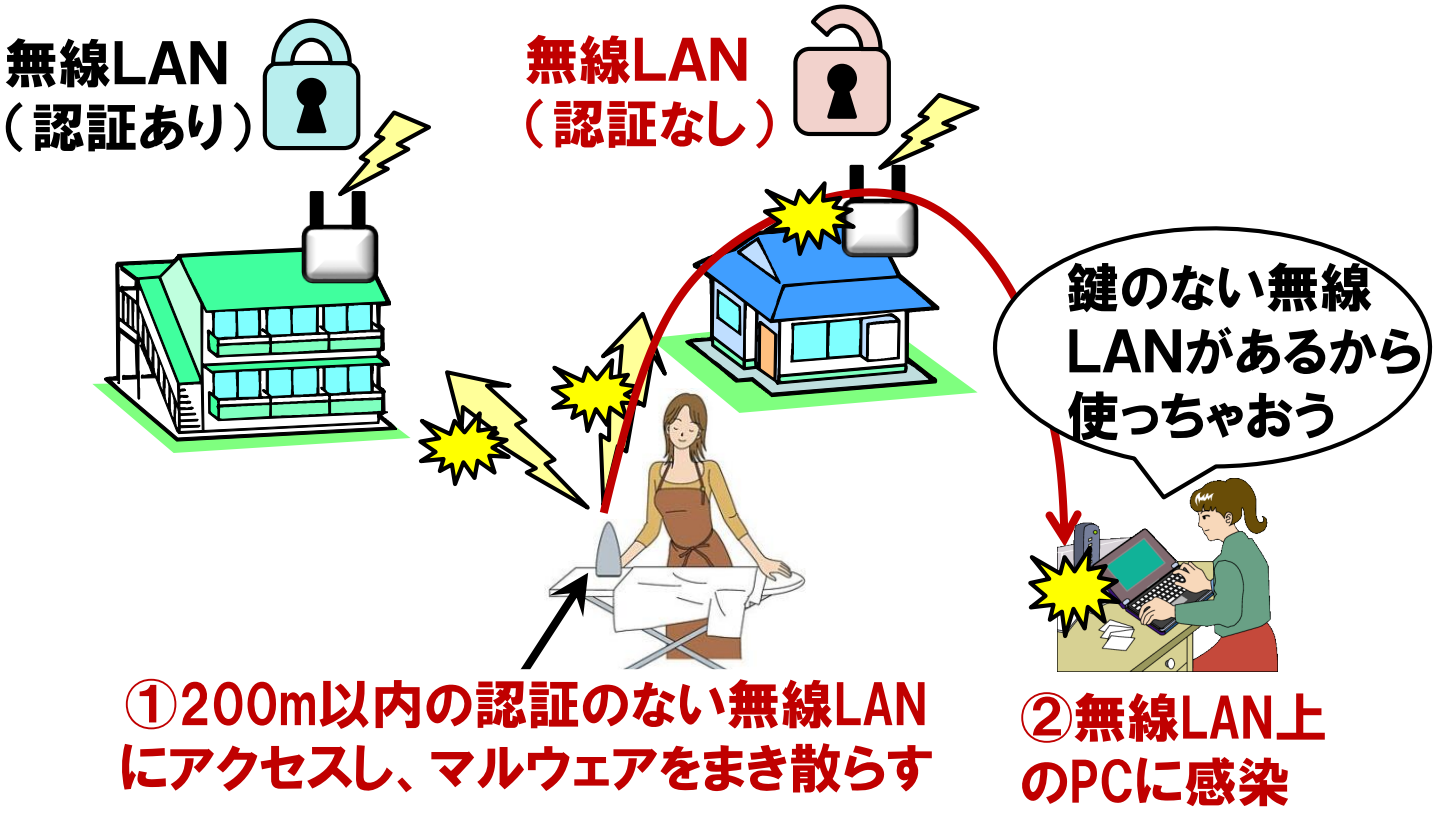
つながる世界のリスクを認識し、安全・安心への対策が急務！

つながる世界のリスク（事例1）

SEC
Software Reliability Enhancement Center

知らないうちに「つながってしまう」

ロシアで、中国製アイロンの中に近隣200m以内の無線LANにアクセスし、ウイルスを撒き散らすチップが埋め込まれていることが発見された。

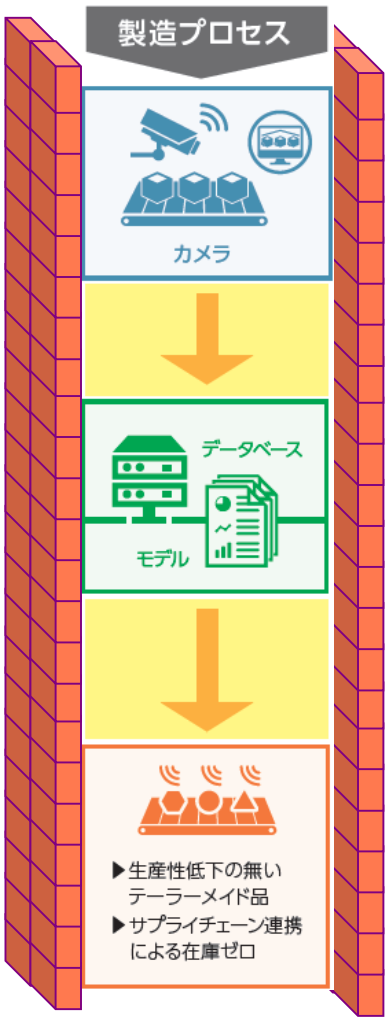


出典：一般社団法人 重要生活機器連携セキュリティ協議会「生活機器の脅威事例集」

つながる世界のリスク(事例2)

SEC Software Reliability Enhancement Center

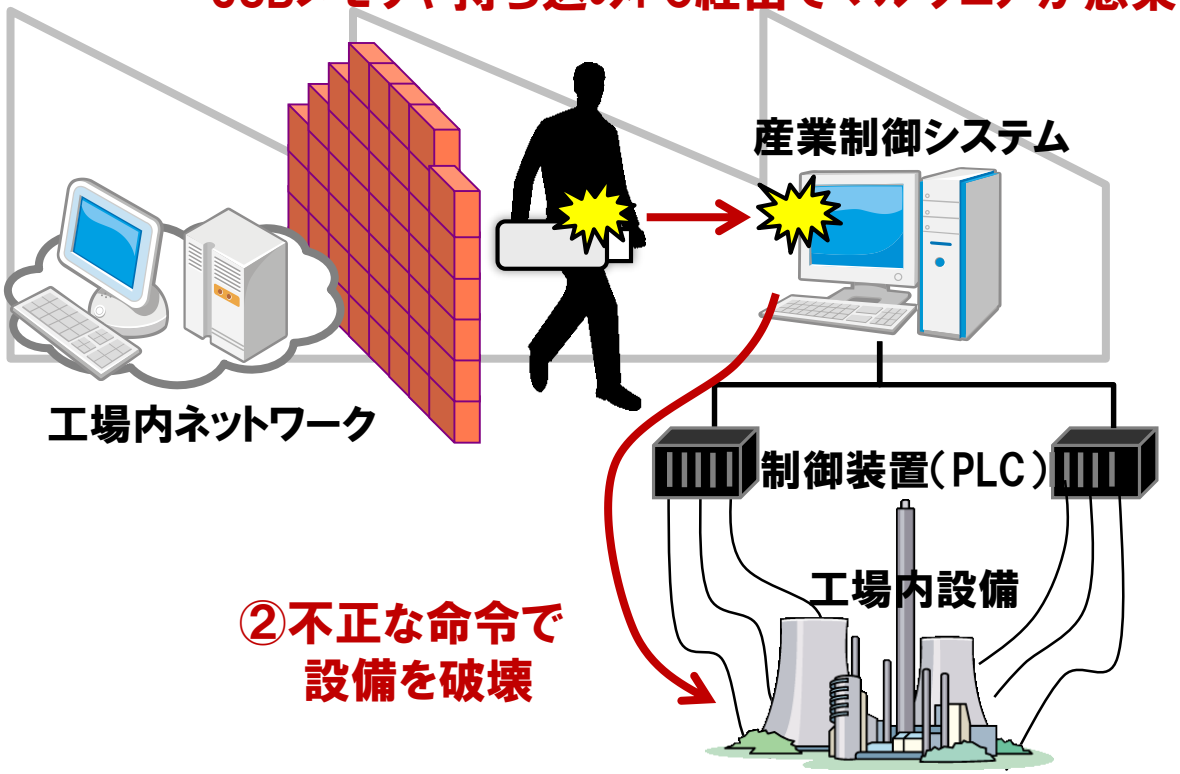
「つながらない」つもりなのに「つながってしまう」



外部に対してクローズなつもりが・・・

ウイルスで工場設備が停止

①ネットワークから隔離されたシステムに
USBメモリや持ち込みPC経由でマルウェアが感染



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「生活機器の脅威事例集」

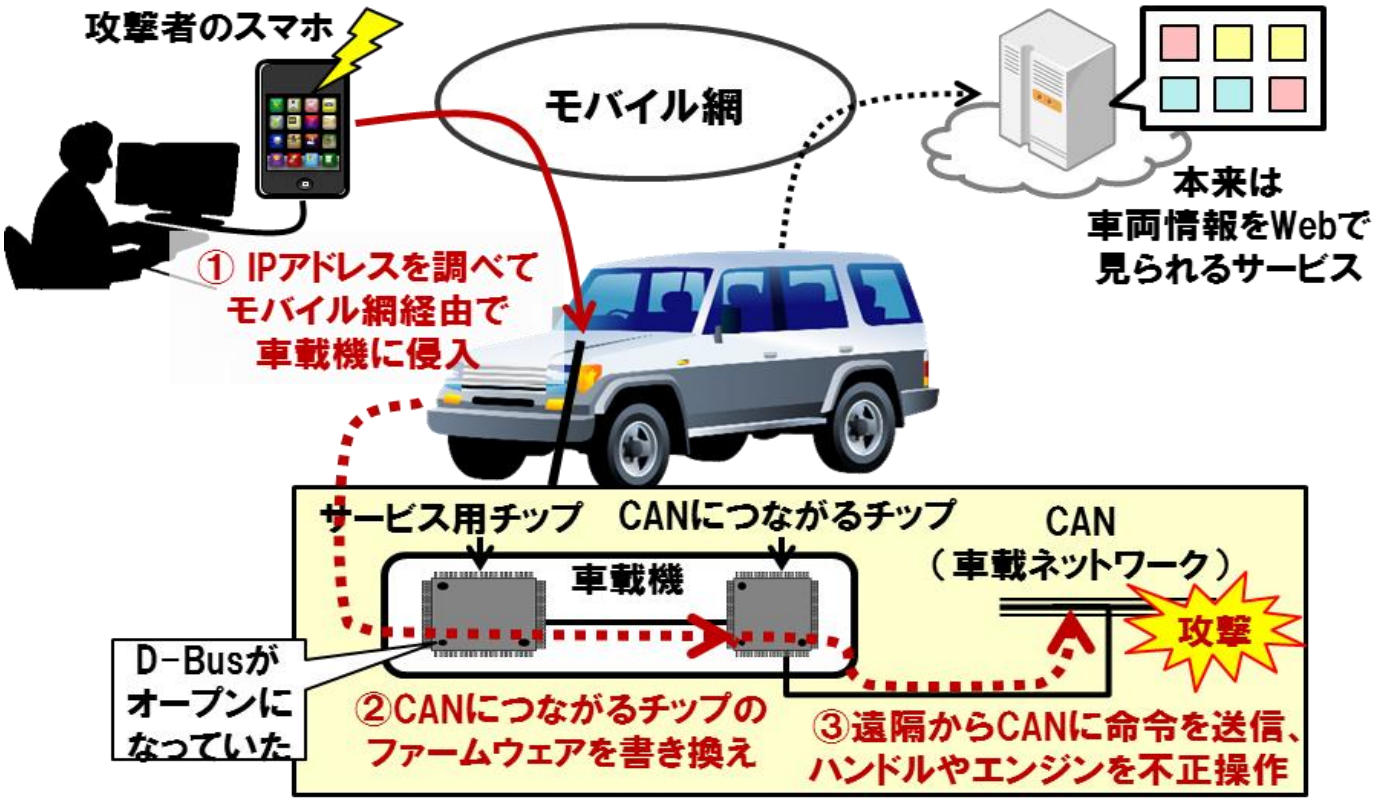
つながる世界のリスク(事例3)

SEC
Software Reliability Enhancement Center

「つながらない」はずが「つながってしまう」

米国blackhat2015で発表があった自動車の攻撃研究事例

スマホから不正に車載器に進入し、ジープのハンドルやエンジンを不正操作した。



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(CCDS)

最近のサイバー攻撃の特徴

SEC Software Reliability Enhancement Center

◆制御システムへの攻撃

事例：発電所を狙った「BlackEnergy」(2015年12月)

ウクライナの発電所が狙われ、州都の一部で大規模な停電が発生。
復旧までに約6時間を要し 40～70万人程度が影響を受けた。
復旧活動を妨害する補助的攻撃も行われた。(遠隔操作・監視の無効化など)

出典：https://www.jpcert.or.jp/present/2016/20160217_CSC-JPCERT01.pdf

◆感染の大規模化

事例：家庭の機器を狙った「Mirai」(2016年9月)

家庭用ルータやネットワーク、デジタルビデオレコーダなどに感染し、
大規模なDDoS攻撃をかける。世界で38万件も感染したともいわれている。
サービスプロバイダーなどが被害に合い、サービス停止に陥った。

出典：https://www.is702.jp/news/2050

◆身代金型の被害

事例：企業や個人を狙った「Ransomware」(2017年5月)

ロンドンの病院などが狙われ、システムが停止した。
ランサムウェアは、コンピューターのファイルにロックをかけ、解除するために
金銭を要求。また、PCの画面をロックし、解除のために金銭を要求する。

出典：http://www.news24.jp/articles/2017/05/13/10361377.html

つながる世界の安全安心の確保に向けた
SECの取組み

つながる世界の安全安心に向けた課題と取組み

SEC Software Reliability Enhancement Center

本日のテーマ

セーフティ&
セキュリティ
設計入門
2015年10月
発行

報告書：分野間実証実験
2017年5月 公開

実証

実践に向けた手引き
2017年6月 発行

具体化

開発指針
2016年5月 発行

拡充

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 発行

課題2：設計手法
セーフティやセキュリティのリスク分析や設計の手法が分からない

課題3：開発指針
経営者や開発者がIoT開発時に考慮すべき事項が分からない

つながる世界の安全安心の実現

課題4：利用時品質
IoTは利用者が多岐にわたり、利用環境も変化、対応への考慮点

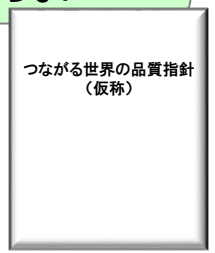
報告書：つながる世界
の利用時の品質
（HCD-Netと共創）
2017年3月 公開

課題1：品質モデル
分野毎に品質の捉え方が異なり、品質に関する議論が出来ない

ソフトウェア品質ガイド
2015年5月 発行

課題5：品質指針
変化が激しいIoTの品質をどう担保すれば良いか分からない

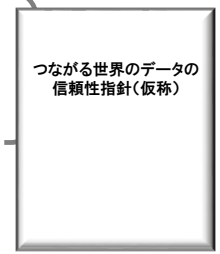
WG実施中



（IVIA,CCDS等と共創）

課題6：データ信頼性
CPSやAIで使うデータ自身の信頼性、信憑性に懸念

計画中



（JASA,MCPC等と共創）

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

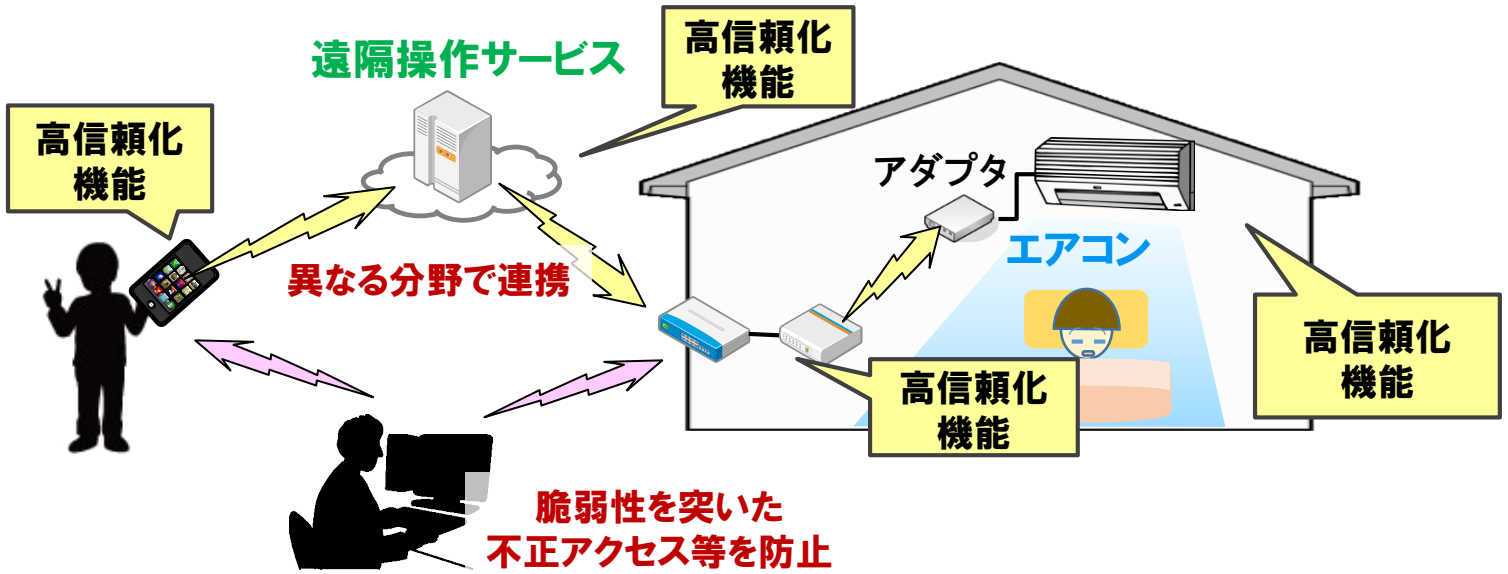
IoTの安全安心のために必要なIoT高信頼化機能

SEC Software Reliability Enhancement Center

■ 「実践に向けた手引き」における用語

■ IoT高信頼化機能とは
IoT機器・システムが相互に連携する（つながる）環境において、**安全安心を確保するための機能**

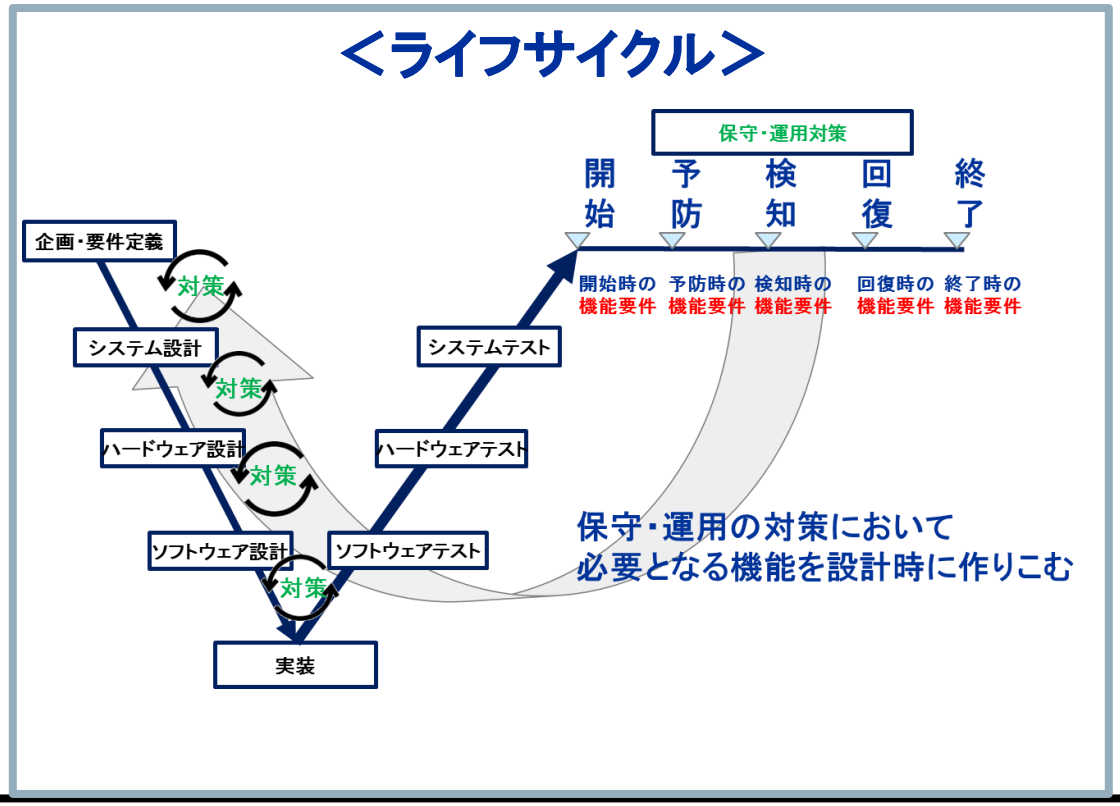
■ IoT高信頼化機能は、様々なIoT機器・システムでの利用を想定

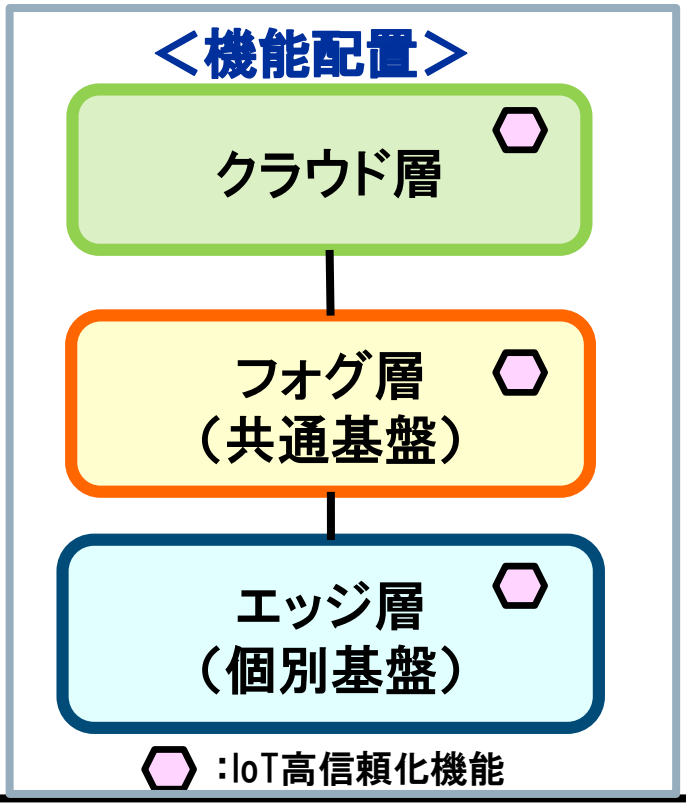


検討のスコープ（ライフサイクルと機能配置）

- 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

障害事例とIoT高信頼化対策

SEC
Software Reliability Enhancement Center

◆障害事例

世界中のネットワークカメラが見放題になっていることを、ロシアのInsecamが公表(2016年1月)
日本国内でも6000台のWEBカメラが見放題に！

◆障害の原因

WEBカメラのパスワードが工場出荷時の初期値のままで、設定してなかった

◆対策例→【機能要件1】

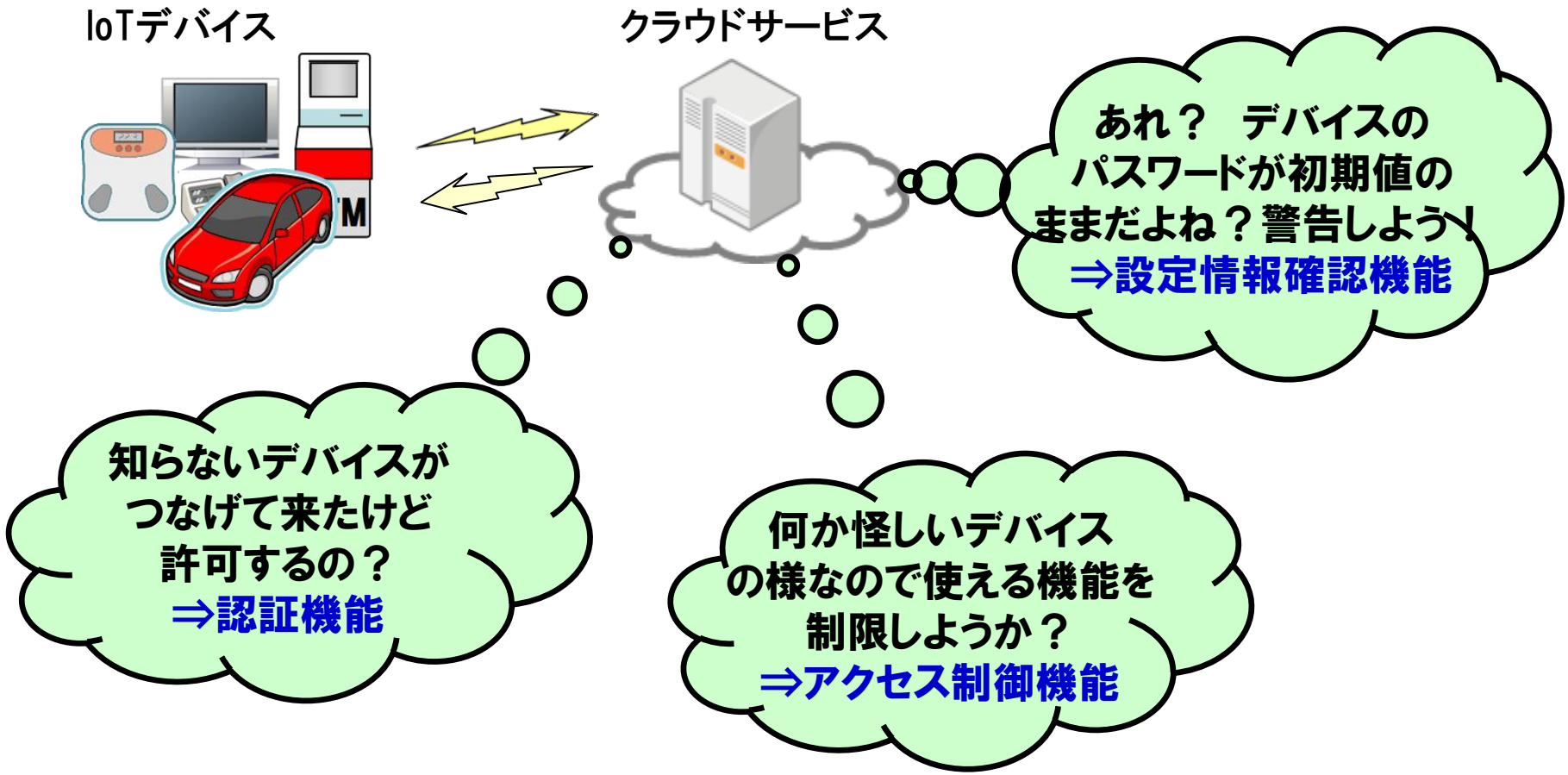
WEBカメラのパスワードの設定状態を確認する機能を設け、初期値の時は警告を発信し、パスワード設定を促す機能を設ける

出典：経済産業省

IoTの高信頼化対策は3つフェーズで考えよう！

SEC Software Reliability Enhancement Center

（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！

SEC Software Reliability Enhancement Center

(2)利用中に守る！(予防、検知、回復の考慮)

IoTデバイス

クラウドサービス

脆弱性の問題が発覚！
早期に予防処置しよう！
⇒構成情報管理機能、
リモートアップデート機能

守るべきモノを特定し
どう守るか対策を入れよう！
⇒ウイルス対策機能、
暗号化機能

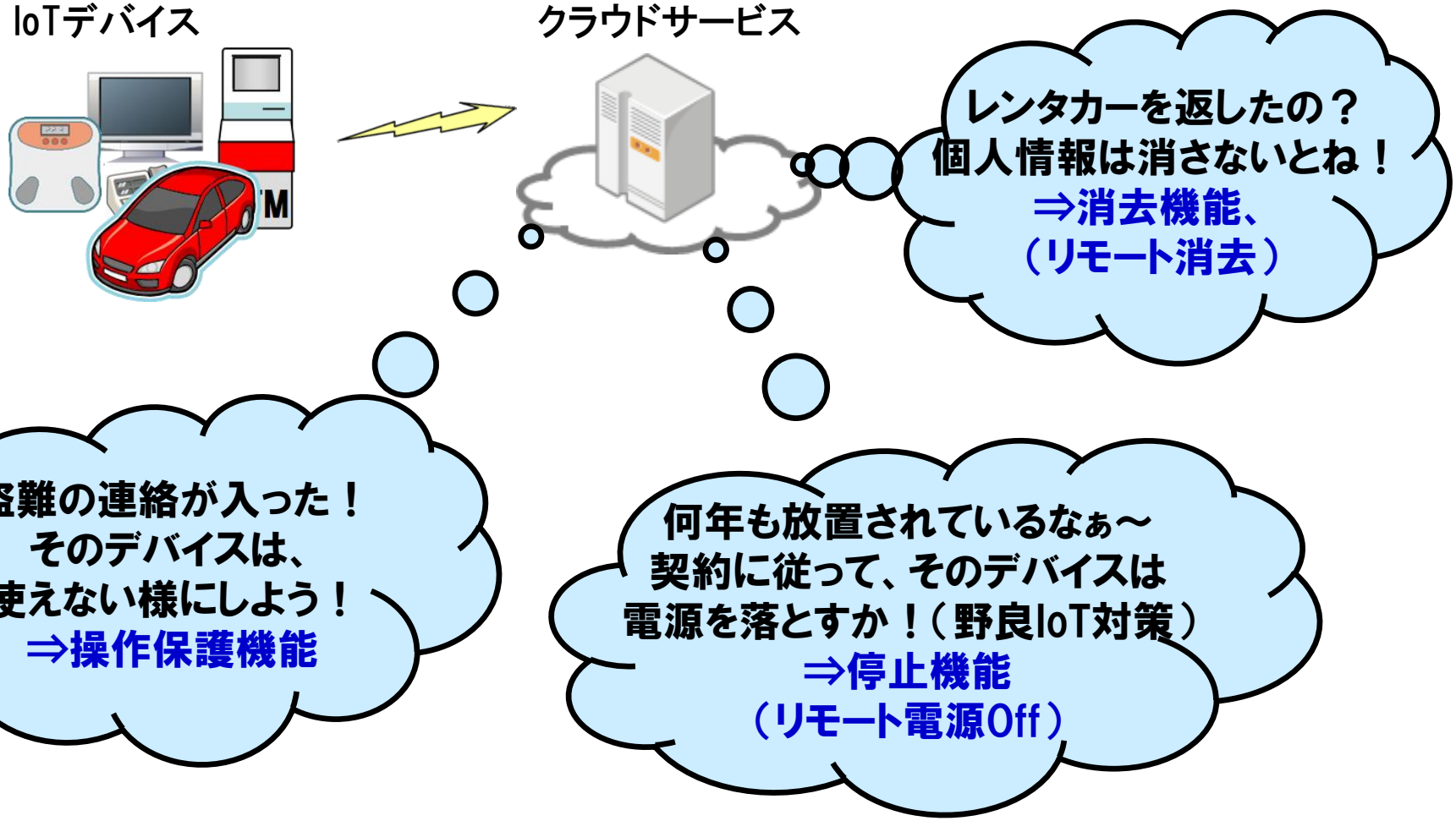
常時、ログを取って、
異常を監視しているし、
定期診断もしているから安心！
⇒ログ収集機能、監視機能
診断機能

何か怪しい振る舞いだなぁ～
乗っ取られた様だ！そのデバイスは
強制停止させよう！
⇒予兆機能、停止機能

IoTの高信頼化対策は3つフェーズで考えよう！

SEC Software Reliability Enhancement Center

(3)利用後も守る！(放置、リユース、廃棄時の考慮)



つながる世界とディペンダビリティ

オープンシステム・ディペンダビリティ(OSD)

現代のコンピュータシステムは常に変化しつづける目的や環境に対応し、未知の障害をマネージし、サービスをできうる限り継続し、障害時には社会に対して説明責任を果たさなければなりません。私たちはこの開放系対応力を「OSD：オープンシステムディペンダビリティ（Open Systems Dependability）」と呼びます。

利用者がシステムに期待する便益を安全にかつ継続的に提供できる

- システム運用開始後の要求の変化に適応できる **（変化対応）**
- システムの障害要因を顕在化する前にできる限り取り除くことができる **（未然防止）**
- 障害が顕在化した後に迅速かつ適切に対応し、影響を最小とすることができる **（障害対応）**

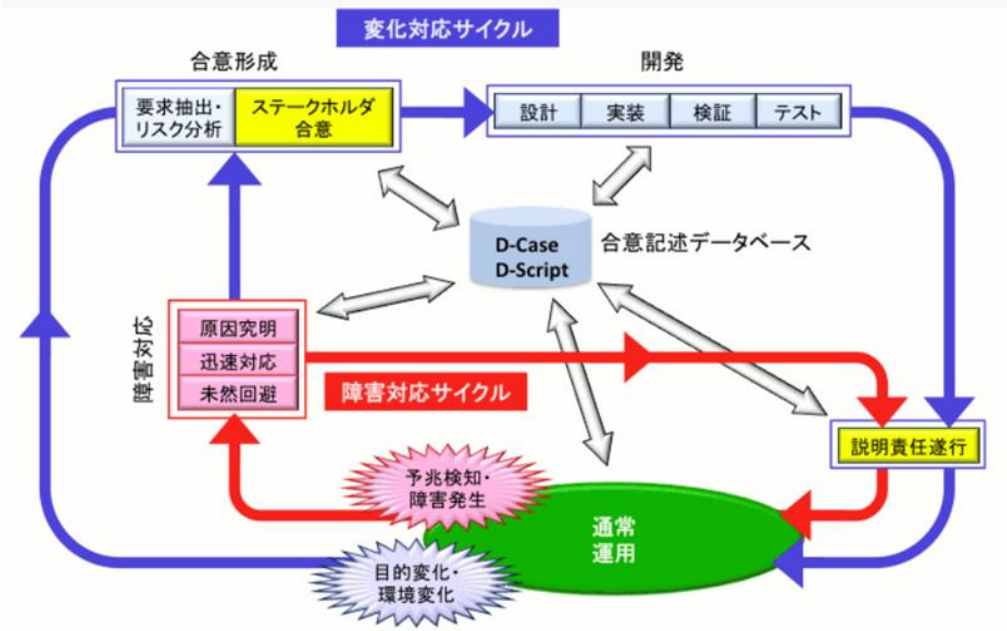
ステークホルダーや社会への説明責任を全うできる

- 全ライフサイクルでの要求と実現に関する合意形成の構造的記録と履歴がある **（合意履歴保持）**
- 合意に基づいたシステムの運用状況の監視と詳細な記録がある **（監視と記録）**

出典：http://deos.or.jp/summary/about_osd-j.html

IoT高信頼化機能の捉え方と同じ方向性を示している

つながる世界とディペンダビリティの関係



出典：http://deos.or.jp/technology/process-j.html

ディペンダブルな世界の実現
（目指すところは同じ）

つながる世界に特化して、
機能レベルに具体化

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

つながる世界の開発指針の今後の展開

「つながる世界の開発指針」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

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との共創活動）(2017/3)**
- IoTの品質確保の検討（IVIA,CCDS等と共創を開始）
- データ品質の検討（JASA,MCPC等と共創予定）

第2版：利用時の品質を製品開発の考慮点に追加(2017/6)

ご清聴ありがとうございました。