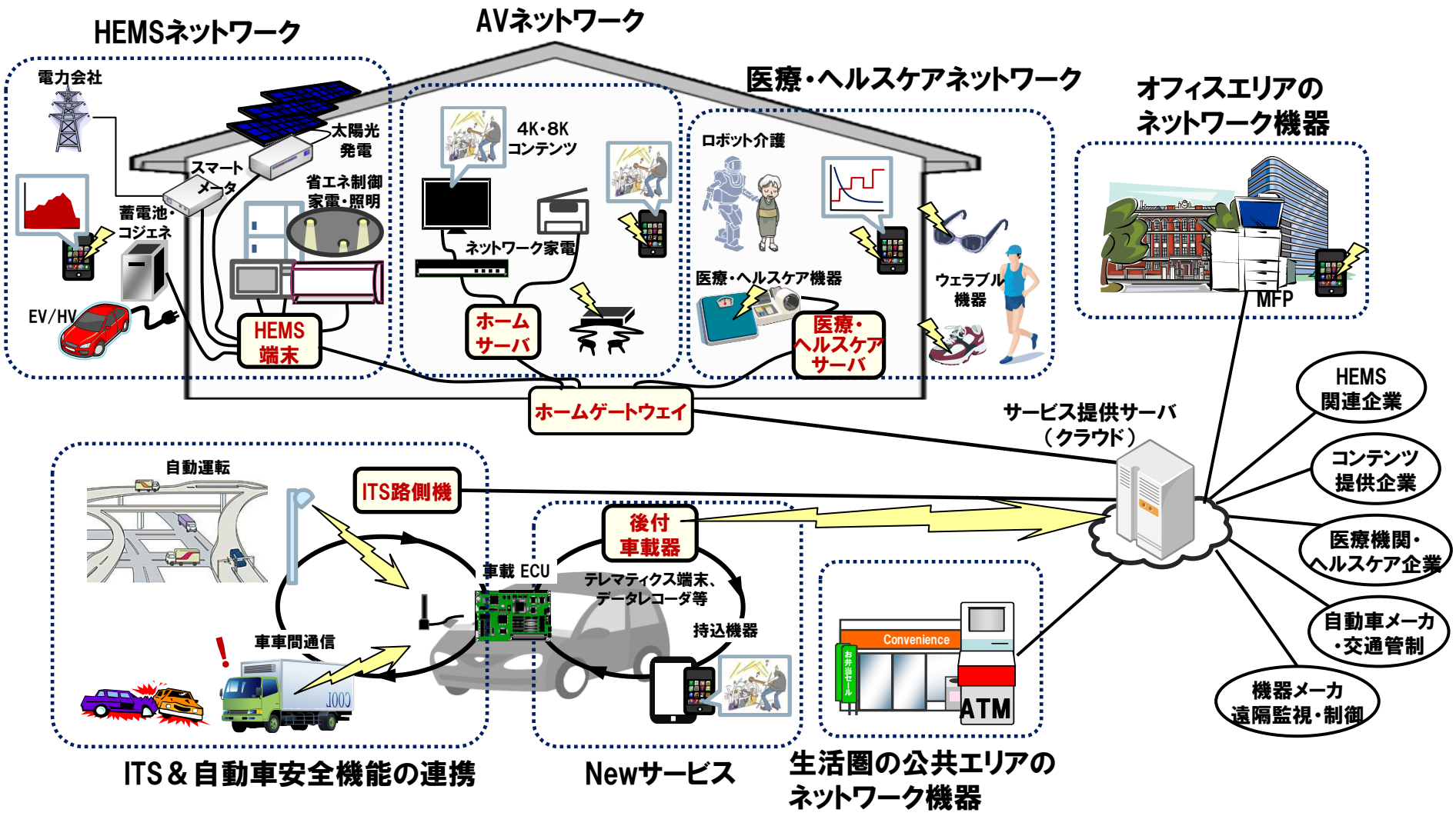
IPA Better Life with IT

「つながる世界の開発指針」の策定の背景と概要

SECセミナー
2016年6月27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)
研究員　宮原 真次

IoT時代：様々なモノやサービスがつながる世界

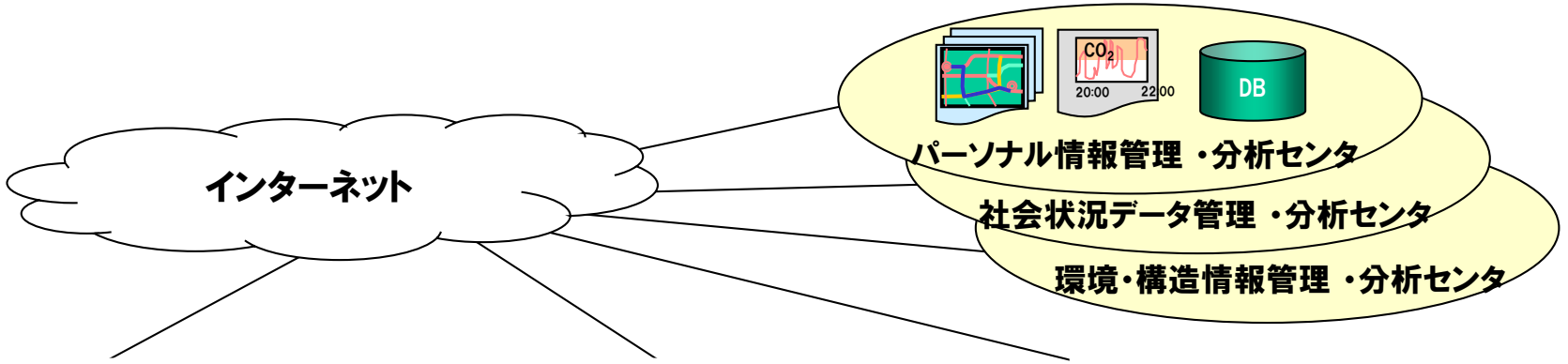


出典：一般社団法人重要生活機器連携セキュリティ協議会 提言

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

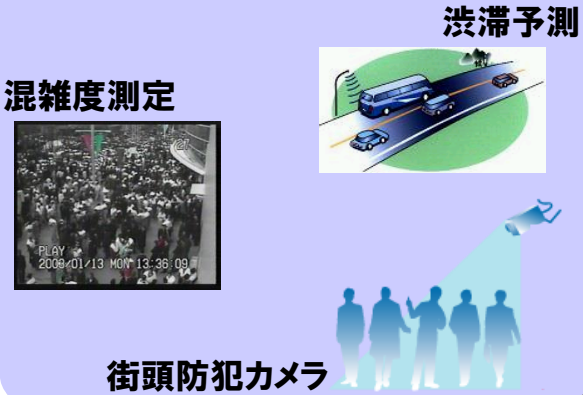
個人から地球環境まで、あらゆるところにセンシングデバイスが遍在する社会が到来。



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

事例1）JR東日本「スマートメンテナンス」

SEC Software Reliability Enhancement Center

センサ・ビッグ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　～

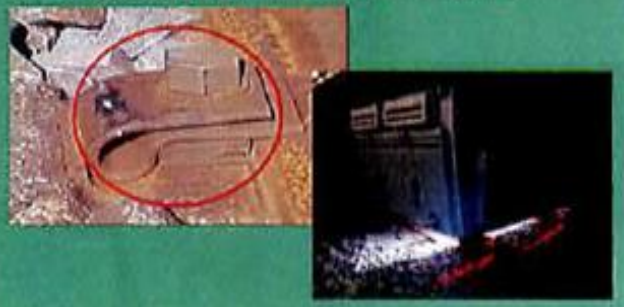
○さらなる安全・安定輸送の確保をめざし、ＩＣＴを活用した業務革新を推進。その一環として、高頻度に線路状態の変化を把握する「線路設備モニタリング装置」 を開発中。

○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。

「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」

■「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

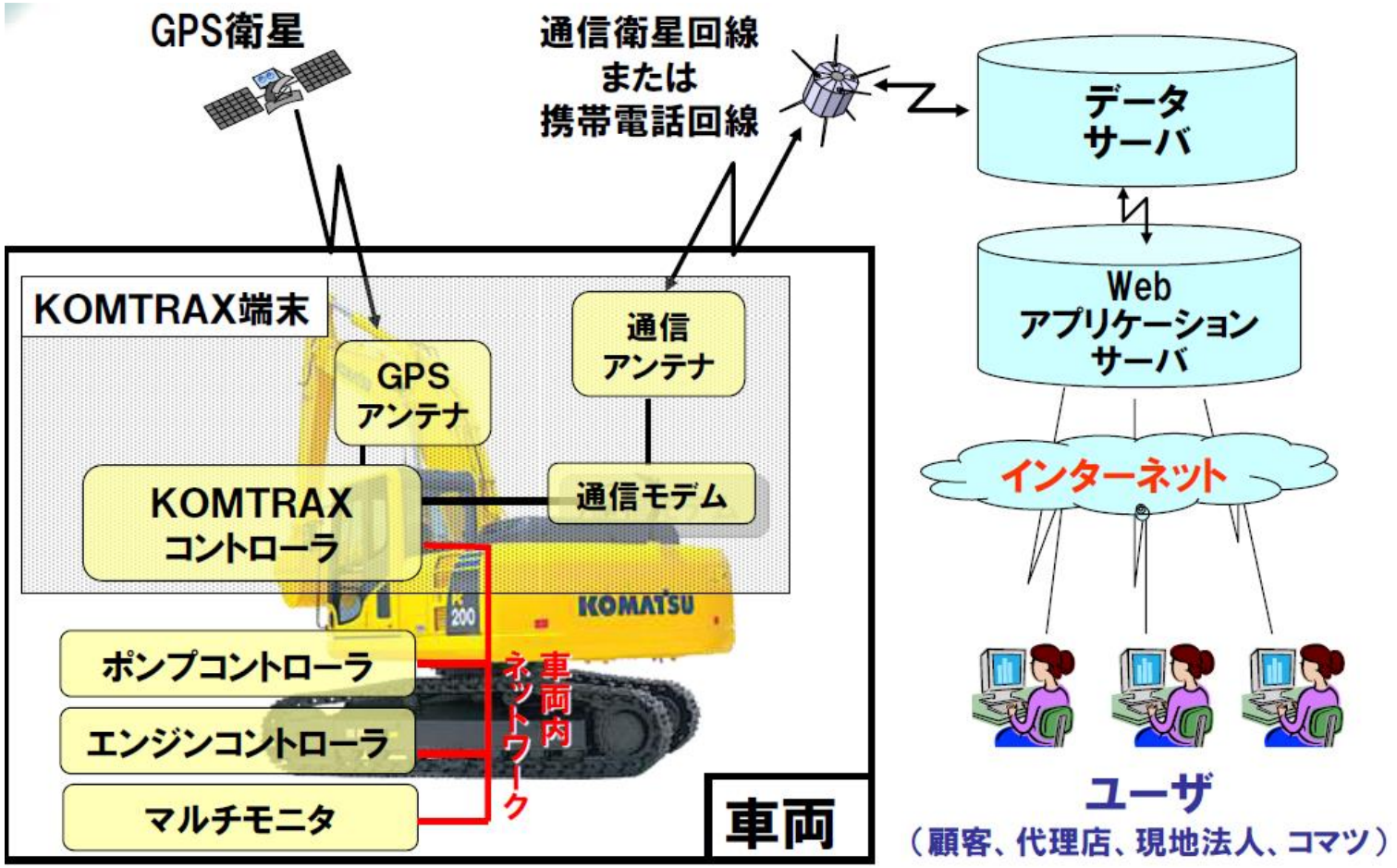
※加速度計とレーザーセンサーにより、線路状態の変化を測定。

出典：JR東日本WEB、ITproニュース2014.8.26記事

事例2)コマツ KOMTRAX

SEC
Software Reliability Enhancement Center

コマツ建機販売は、世界中の建設機械の場所や稼働状況を遠隔から確認できるサービスを提供(1999年から本格販売)。IoTの先駆け事例。



出典:中部経済産業局セミナー(2014年) コマツプレゼン資料

事例3)バルセロナ市の公共IoT（スマートパーキング）

バルセロナ市では、市内全域にWi-Fiで接続したスマートパーキング
メータを配置して、住民に駐車可能な地点の情報をリアルタイムで提供。
また、スマートフォンでの駐車料金の支払いを可能としている。

Figure 8.2 Installation and control interface of a Smart Parking application

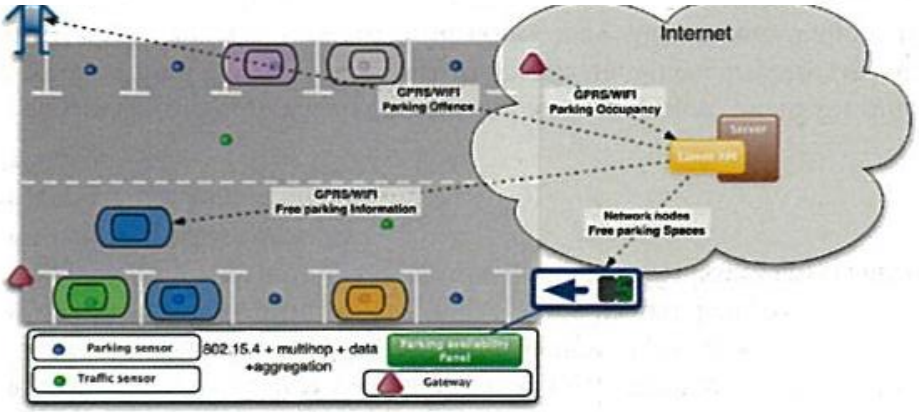


Figure 8.1 Architecture of the parking space availability control service

Figure 8.9 Picture of the selected Smart Parking test facility

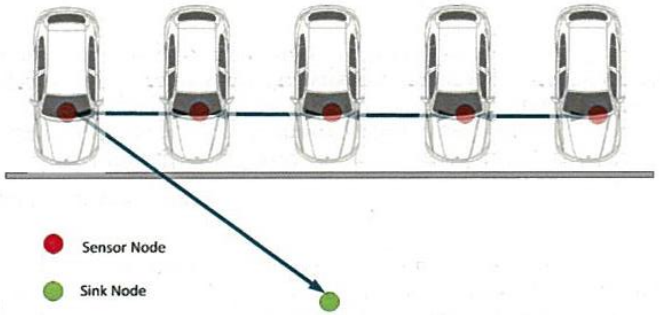
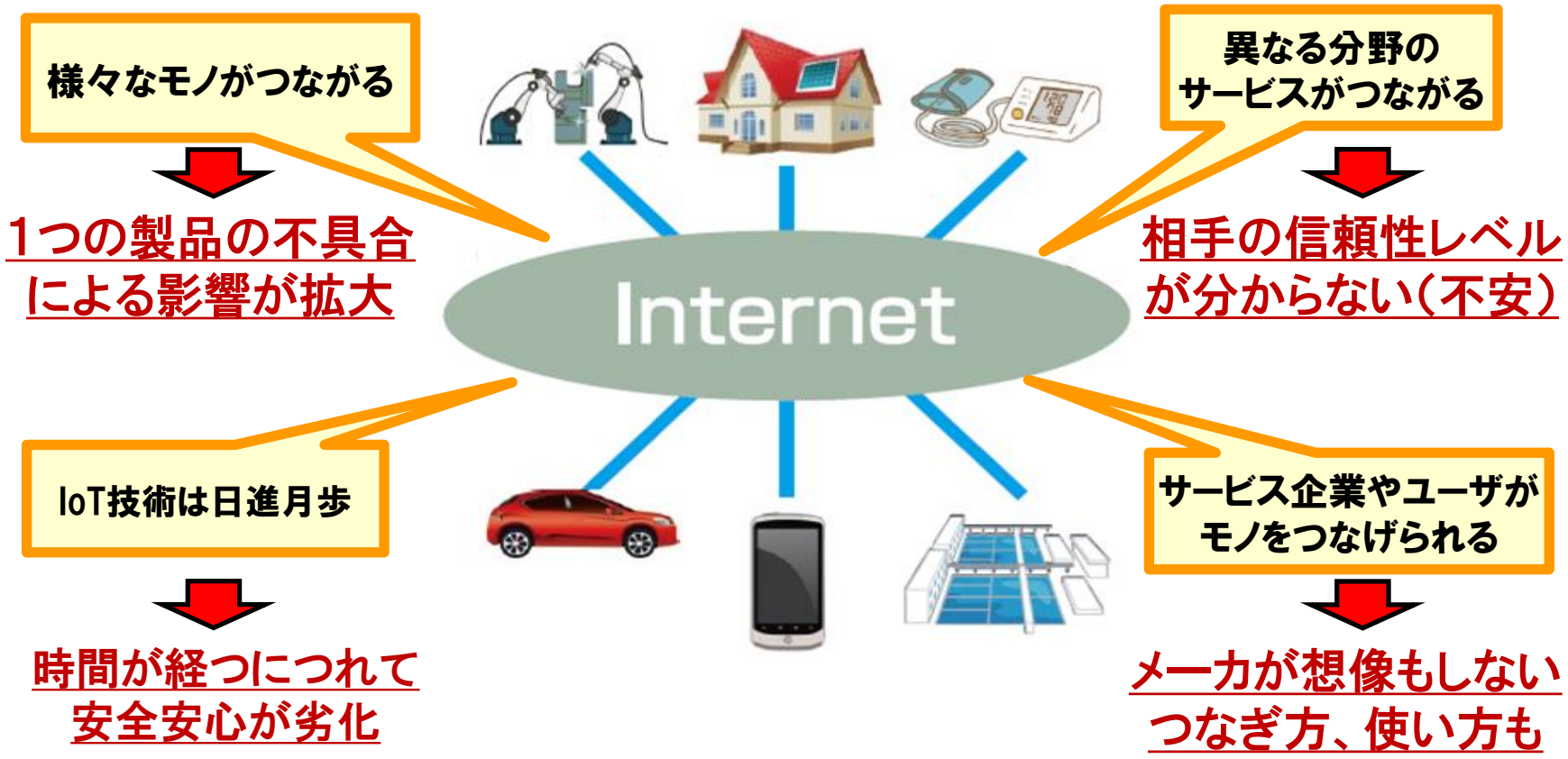


Figure 8.10 Configuration of the network topology

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



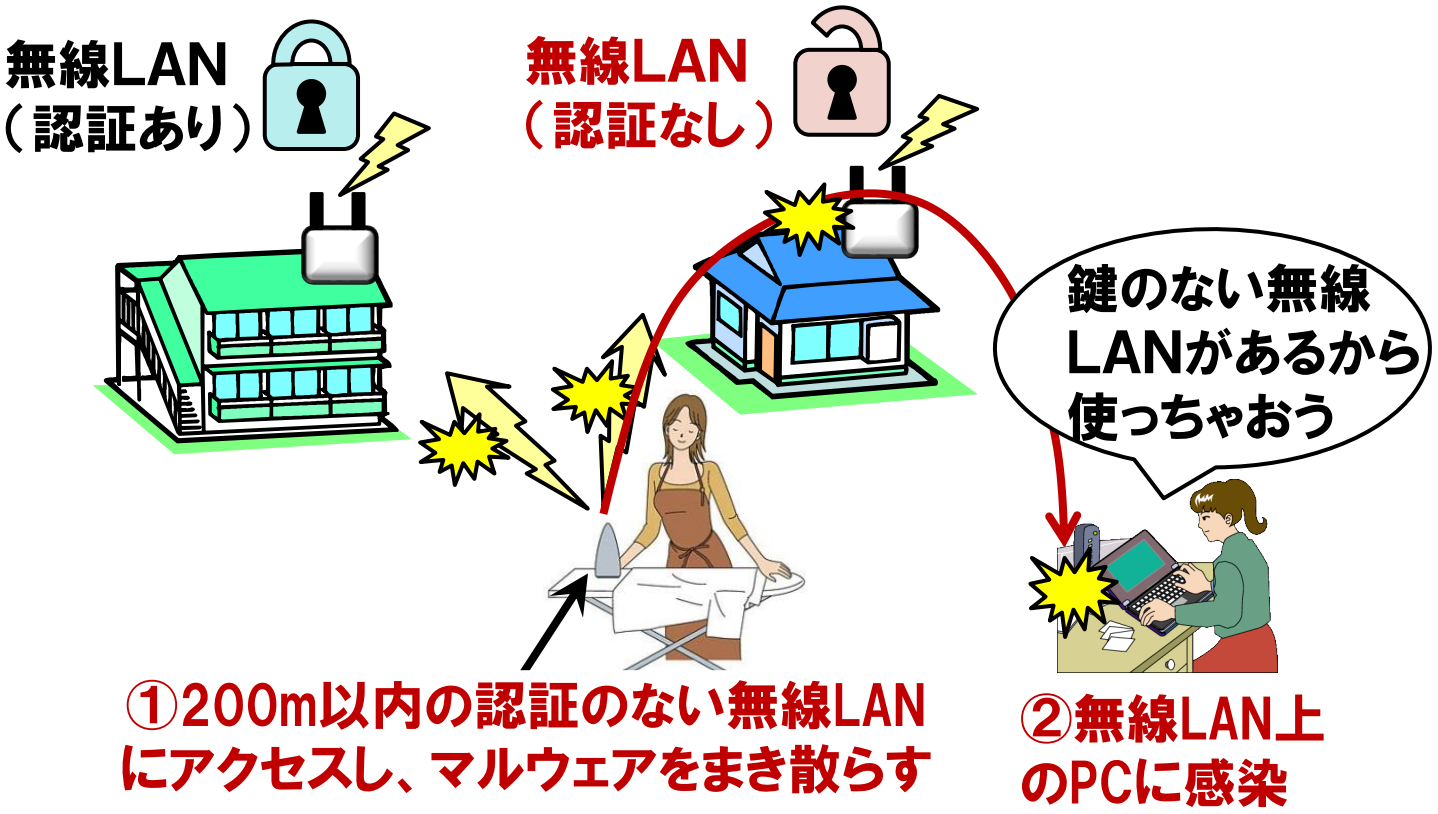
つながる世界のリスクを認識し、安全・安心への対策が急務！

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。

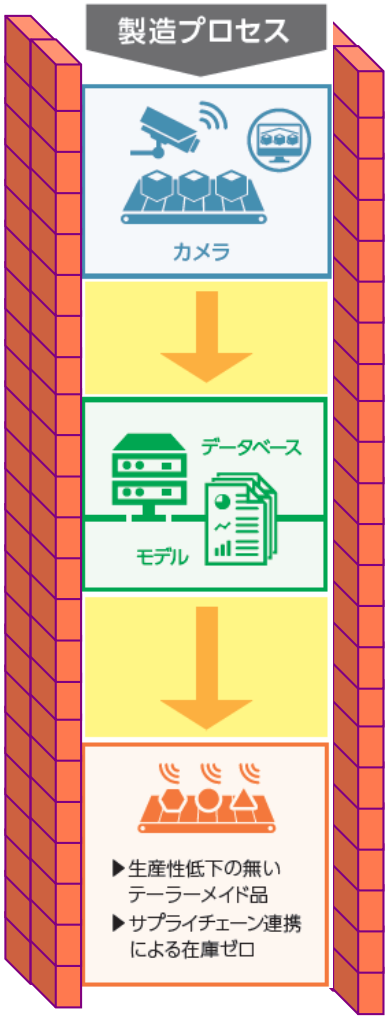


出典:一般社団法人 重要生活機器連携セキュリティ協議会「生活機器の脅威事例集」

つながる世界のリスク(事例2)

SEC Software Reliability Enhancement Center

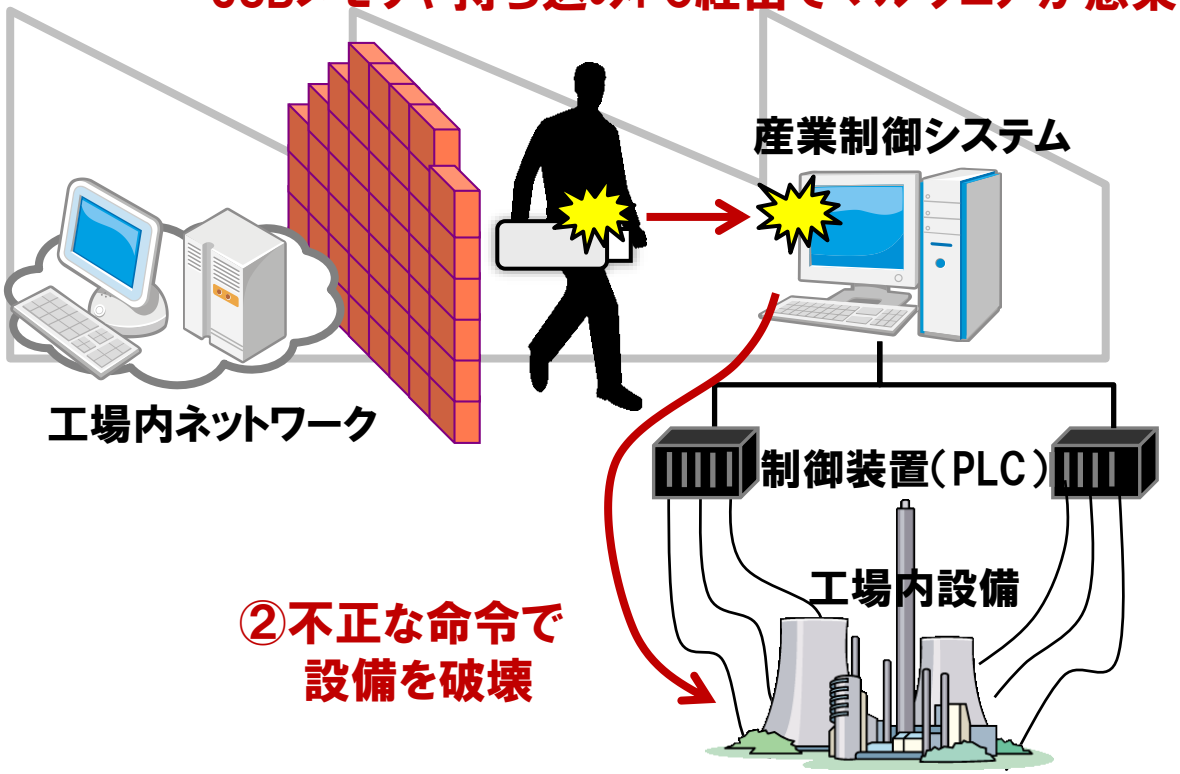
「つながらない」つもりなのに「つながってしまう」



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



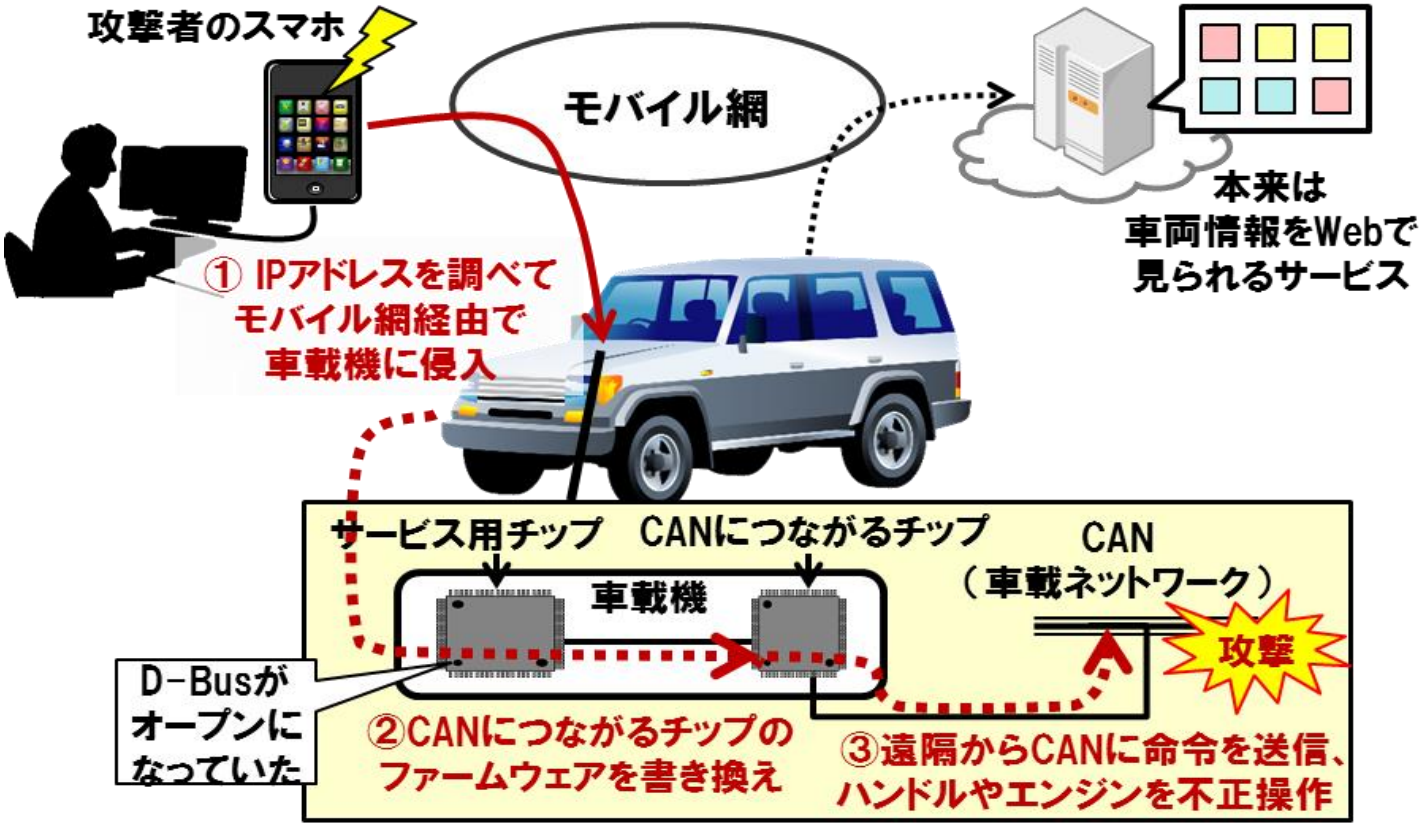
出典:一般社団法人 重要生活機器連携セキュリティ協議会「生活機器の脅威事例集」

つながる世界のリスク(事例3)

SEC
Software Reliability Enhancement Center

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)

つながる世界の開発指針の狙い

例）

想定されるリスク

- 車を制御・操作中のスマホのハングアップにより、制御・操作が効かなくなり、重大な事故が発生
- 脆弱性がある側の機器への不正アクセスにより、相手側の機器に保存されている情報が盗難　等

IoT時代の安全と安心への危惧

つながる事を想定した安全･安心に向けた設計が重要に！

つながる世界の開発指針検討WG

SEC
Software Reliability Enhancement Center

- ◆ 産業界や学会の有識者で構成したWGをH27年8月に立ち上げ
- ◆ IoT製品・システムの開発時に考慮すべき、リスクや対策を検討

つながる世界の開発指針検討WG委員一覧

役割	委員氏名	所属先名
主査	高田　広章	名古屋大学
副主査	後藤　厚宏	情報セキュリティ大学院大学
委員	飯島　雅人	株式会社ミサワホーム総合研究所
委員	緒方　日佐男	日立オムロンターミナルソリューションズ株式会社
委員	荻野　司	一般社団法人 重要生活機器連携セキュリティ協議会
委員	奥原　雅之	富士通株式会社
委員	梶本　一夫	パナソニック株式会社
委員	木村　利明	一般財団法人　機械振興協会　技術研究所
委員	高橋　裕一	株式会社日立製作所　情報・通信システム社
委員	長谷川　勝敏	一般社団法人組込みイノベーション協議会
委員	早川　浩史	株式会社デンソー
委員	松並　勝	一般社団法人日本スマートフォンセキュリティ協会
委員	三上　清一	株式会社JVCケンウッド

つながる世界の開発指針を策定

つながる世界の開発指針の特徴

■安全・安心なIoTを実現するために、IoT製品やシステムの開発者が開発時に考慮すべきリスクや対策を17の指針として明確化

■IoTに関連する様々な製品分野・業界において分野横断的に活用されることを想定

■IoT製品・システムの安全性・セキュリティに関して分野横断的に活用可能な国内初の開発指針

※本開発指針は、2016年3月24日に公開
http://www.ipa.go.jp/sec/reports/20160324.html

IoT関連の国際規格類

SEC Software Reliability Enhancement Center

	規格/団体	概要	主要参加メンバー等
共通・汎用規格	IEEE　P2413	IoTにおいてドメイン横断のプラットフォームを検討	-
	ISO/IEC 30141	JTC1　SWG5の後をうけてWG10でリファレンスアーキテクチャを検討	-
	NIST CPS PWG	CPSのFramework検討のためのPublic WG	-
	oneM2M	世界の主要7標準化団体の共同プロジェクト。従来の垂直統合型M2Mサービスを共通PFで水平統合型に展開	Continua、HGI、OMA等業界団体約200社
代表的な業界別・特定規格	Industrie 4.0	ドイツ政府が製造業のイノベーション政策として主導	Siemens 、Bosch 、SAP 、他
	IIC	エネルギー、医療、製造、運輸、行政に焦点	GE、AT&T、IBM、Cisco、Intel等、約150社
	AllSeen Alliance	家電製品、モバイル端末向け規格	Qualcomm 、LG 、MS 等 、約50社
	OCF	家庭、企業における多様なデバイス間の相互運用のための規格	Intel 、サムスン電子 、Cisco、MS、他
	HomeKit	iOS（スマホ）と機器をつなぐ規格	Apple、他約20社

開発指針の策定方針

SEC
Software Reliability Enhancement Center

IoT共通・汎用規格
（安全安心関連項目）

共通・汎用的であり
実践レベルまで踏み込んでない

業界別・特定規格
（安全安心関連項目）

業界特性に依存する部分が多い

参考

本開発指針

実践レベルまで踏み込みつつ
共通的な対策案としてまとめる

普及展開

収集

実践的リスク例

リスク対策

つながる世界の開発指針（17個）

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（ライフサイクルでの考慮点）

◆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指針）
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

開発指針の「方針」の解説

SEC Software Reliability Enhancement Center

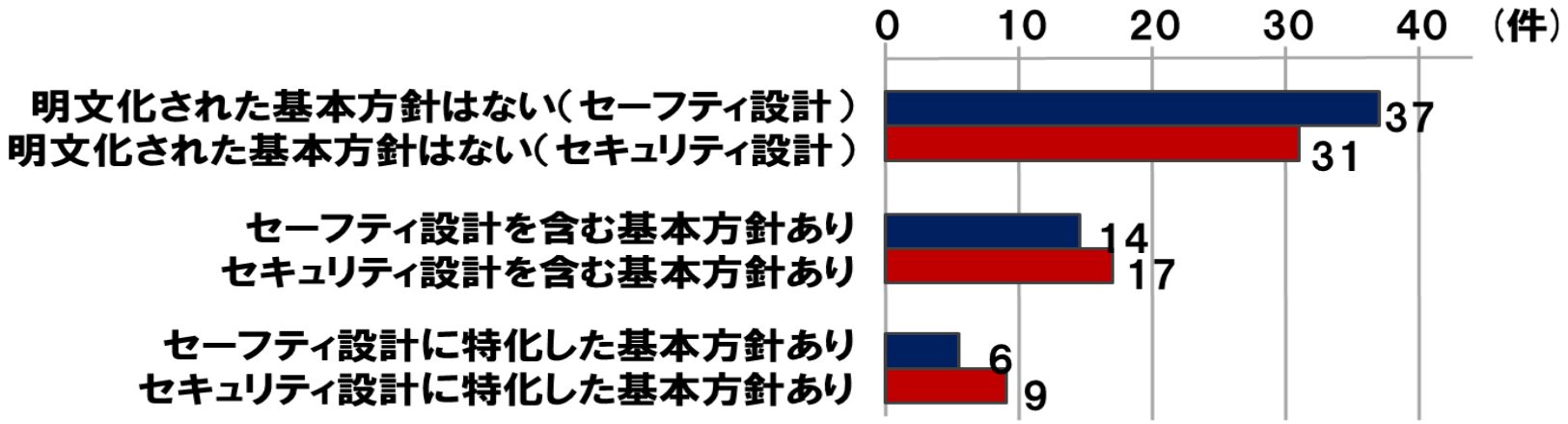
◆ 方針：つながる世界の安全安心に企業として取り組む

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」の解説

◆ 分析：つながる世界のリスクを認識する

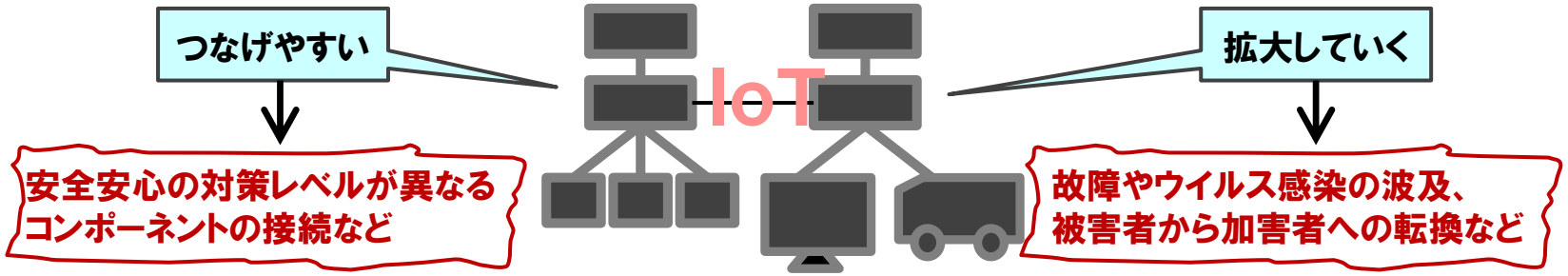
IoTの世界では、つながっていなかったモノがつながることで想定外の問題が発生することや障害が波及するリスクなど検討する必要がある。

守るべきものを特定

つながることによるリスクの想定

つながりで波及するリスクの想定

物理的なリスクを認識



開発指針の「設計」の解説

SEC Software Reliability Enhancement Center

◆ 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、全体で守ることも重要。また、障害が波及しない仕組みや接続相手の信用を確認する仕組みも重要。

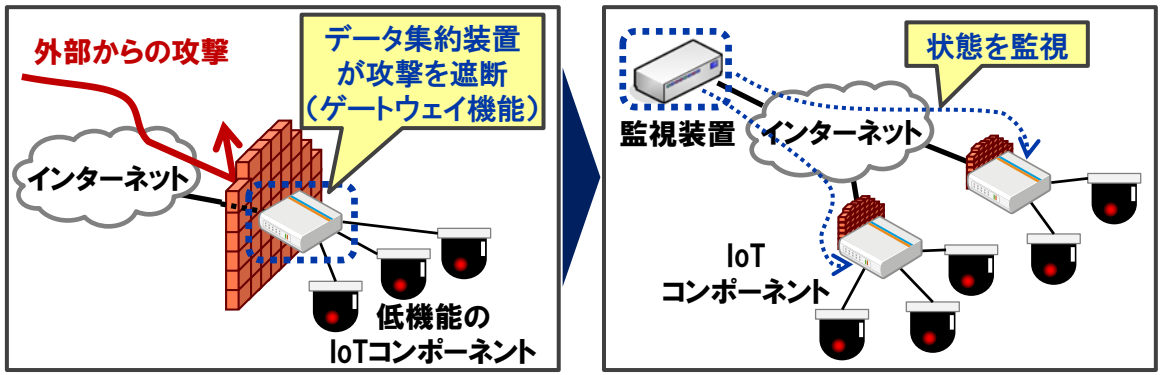
個々でも全体でも守る

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」の解説

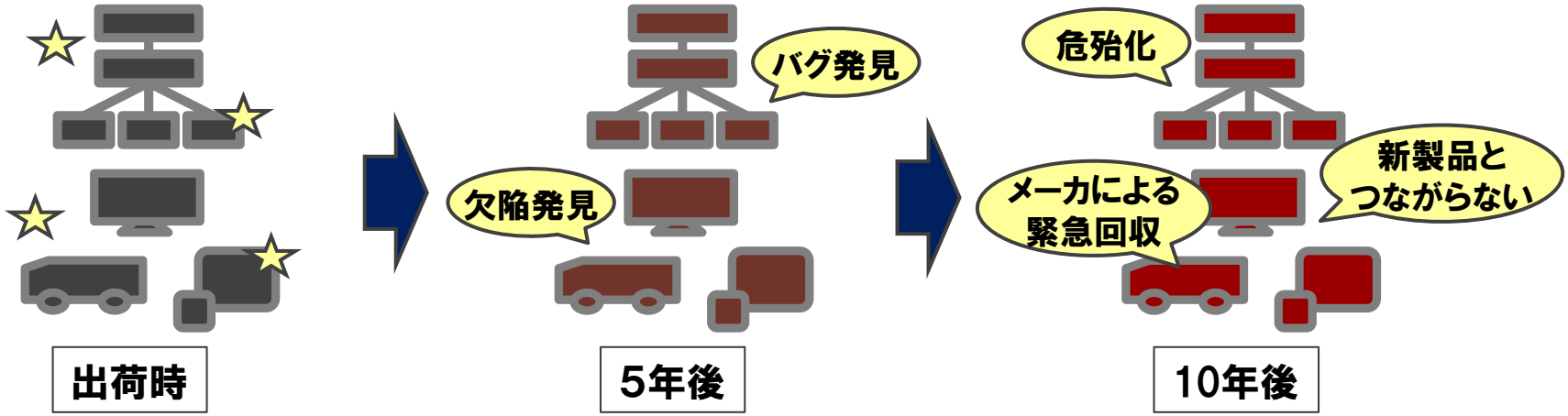
SEC
Software Reliability Enhancement Center

◆ 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」の解説

SEC Software Reliability Enhancement Center

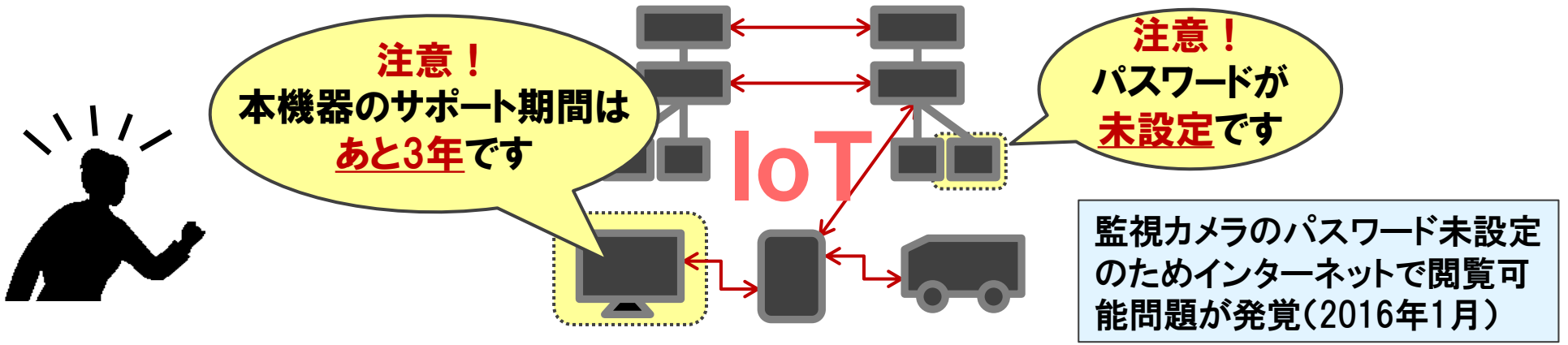
◆運用：関係者と一緒に守る

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になる。

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



開発指針の記述内容の例

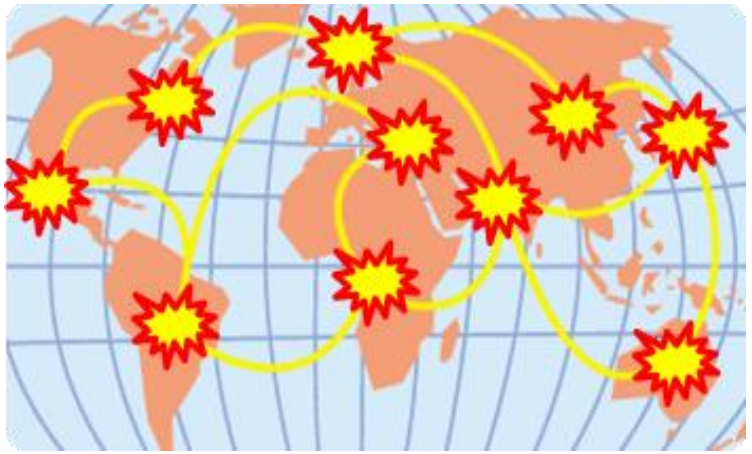
SEC
Software Reliability Enhancement Center

指針

指針6　つながりで波及するリスクを想定する

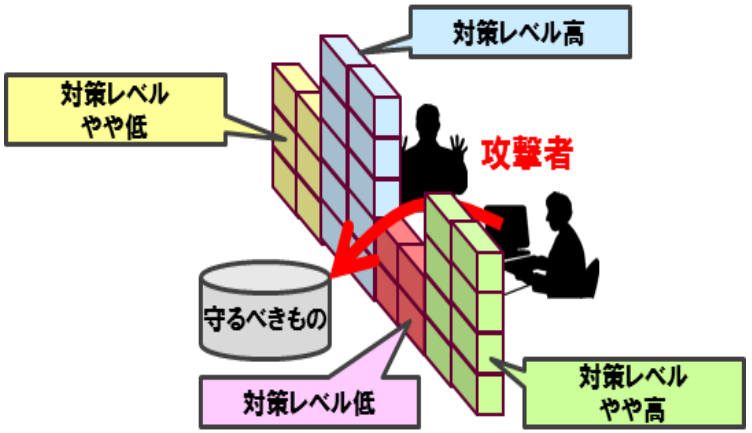
ポイント

①セキュリティ上の脅威や機器の故障の影響が、他の機器とつながることにより波及するリスクを想定する。



ポイント

②特に、安全安心対策のレベルが低い機器やシステムがつながると、影響が波及するリスクが高まることを想定する。



開発企業における開発指針の使い方

SEC Software Reliability Enhancement Center

◆ 開発指針の利活用方針

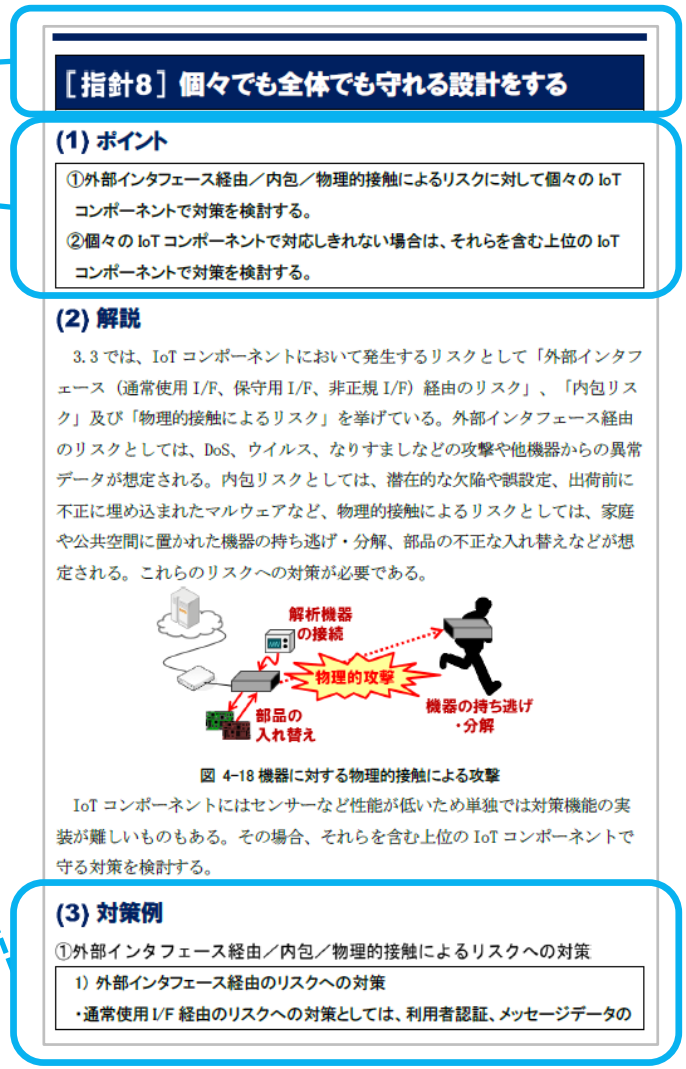
開発指針

各指針のポイントは必ず検討すべき内容

対策の実施は当事者の判断とする。実施する場合は各指針の対策例が参考となる

◆ 開発指針の利活用方法

- IoT製品やシステムの開発時のチェックリストとして利用する。
- 指針で記述している事項は、検討時に企業や団体、業界の実情に合わせてカスタマイズして利用する。
- 内部での開発のみならず受発注の要件確認にも活用する。
- チェック結果を取組みのエビデンスとして活用する。



［指針8］個々でも全体でも守れる設計をする

(1) ポイント

①外部インタフェース経由／内包／物理的接触によるリスクに対して個々の IoT コンポーネントで対策を検討する。
②個々の IoT コンポーネントで対応しきれない場合は、それらを含む上位の IoT コンポーネントで対策を検討する。

(2) 解説

3.3 では、IoT コンポーネントにおいて発生するリスクとして「外部インタフェース（通常使用 I/F、保守用 I/F、非正規 I/F）経由のリスク」、「内包リスク」及び「物理的接触によるリスク」を挙げている。外部インタフェース経由のリスクとしては、DoS、ウイルス、なりすましなどの攻撃や他機器からの異常データが想定される。内包リスクとしては、潜在的な欠陥や誤設定、出荷前に不正に埋め込まれたマルウェアなど、物理的接触によるリスクとしては、家庭や公共空間に置かれた機器の持ち逃げ・分解、部品の不正な入れ替えなどが想定される。これらのリスクへの対策が必要である。

図 4-18 機器に対する物理的接触による攻撃

IoT コンポーネントにはセンサーなど性能が低いため単独では対策機能の実装が難しいものもある。その場合、それらを含む上位の IoT コンポーネントで守る対策を検討する。

(3) 対策例

①外部インタフェース経由／内包／物理的接触によるリスクへの対策

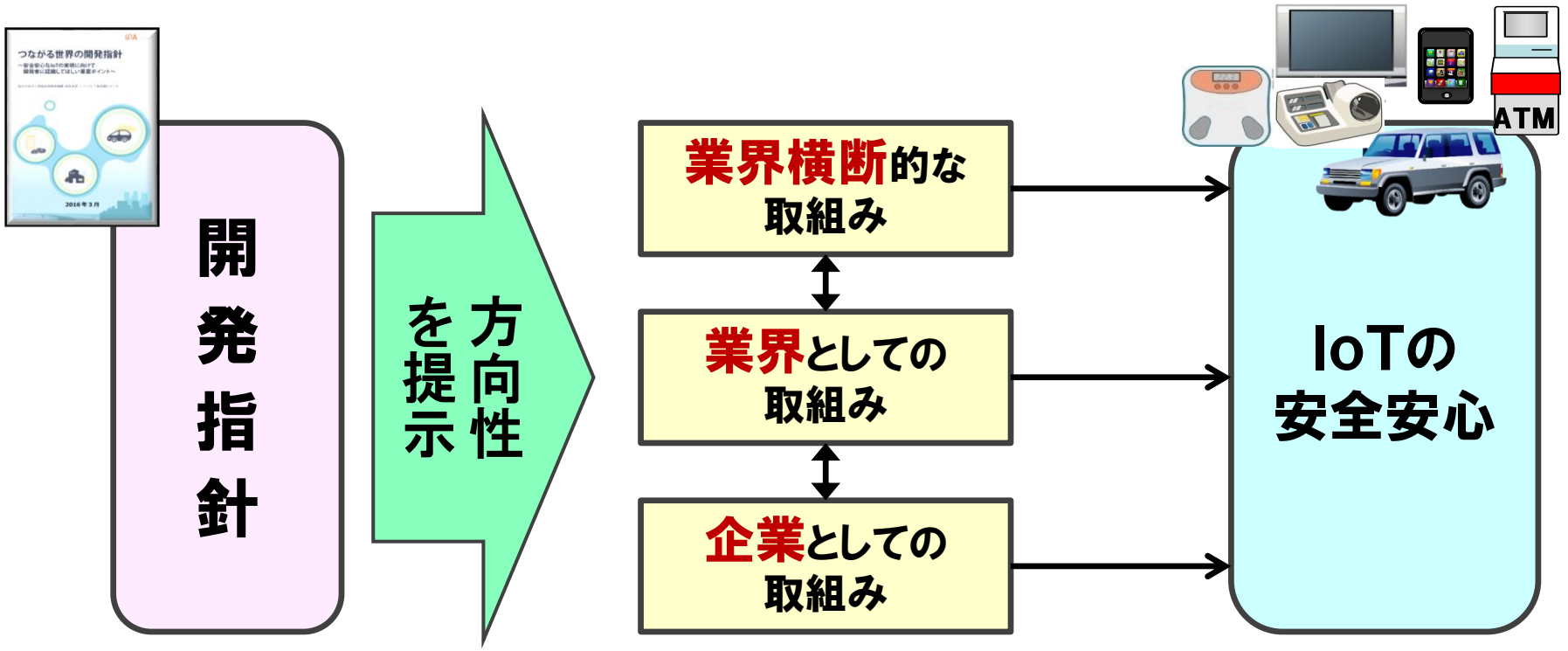
1) 外部インタフェース経由のリスクへの対策
・通常使用 I/F 経由のリスクへの対策としては、利用者認証、メッセージデータの

開発指針の普及展開

SEC Software Reliability Enhancement Center

◆ 産業界や国のIoT政策への働きかけ

分野横断的に活用されることを想定し、方向性を提示（抽象度が高い）
→　各企業や業界での詳細化を期待（産業界やIoT政策に働きかけていく）



つながる世界の開発指針に関わる実証実験

SEC
Software Reliability Enhancement Center

◆目的

開発指針のリスク対応策として考えられる技術の中で、まだ、未確立な以下の技術に関して、実装の可能性を実証する。(FA分野での実験)

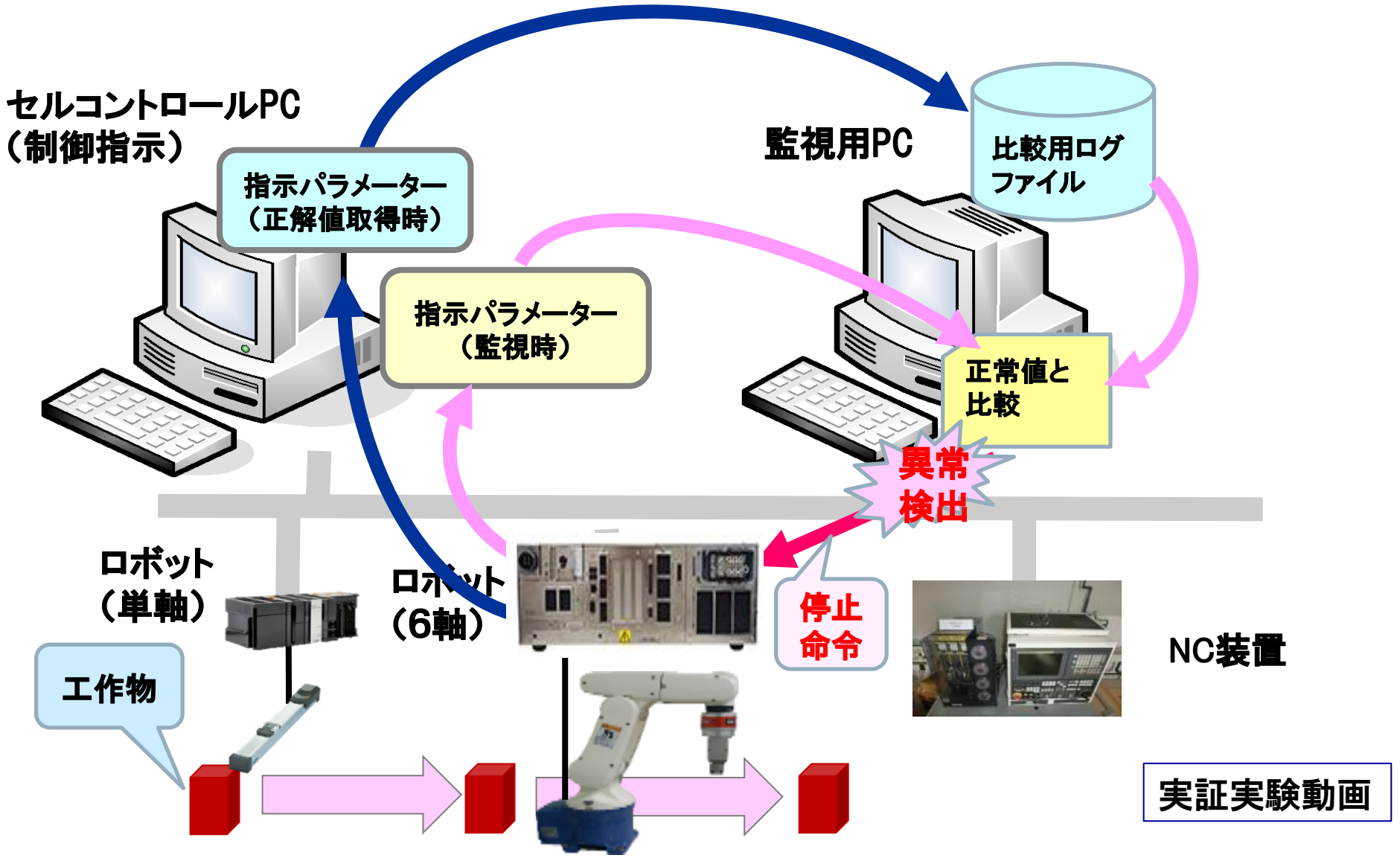
- 障害の波及防止の対策技術【指針9に相当】
- 相互接続時の信頼性確認技術【指針11に相当】

◆期間:2015年12月7日～2017年3月31日 (報告書は、2016年5月11日公開済)

http://www.ipa.go.jp/sec/reports/20160511_3.html

◆体制
- IPA:実証実験の仕様決定、評価と報告書作成
- ORiN協議会:ORiNソフトウェアへの実験機能の追加
- 機械振興協会:実験環境の提供(技術研究所(東久留米))

実証実験での波及防止の原理と実験映像



【参考】IoTセキュリティガイドラインへの展開

SEC Software Reliability Enhancement Center

政府のIoT政策として、IoT推進コンソーシアムで策定した「IoTセキュリティガイドライン」に「つながる世界の開発指針」が採用された。

IoTセキュリティガイドライン（パブコメ公開版）

1.5 ガイドラインの全体構成

第 1 章においては、本ガイドラインの背景や目的、ガイドラインの対象とする IoT、そして対象読者を示した。

第 2 章においては、以下に記載するとおり、IoT 機器・システム、サービスの供給者である経営者、機器メーカ、システム提供者・サービス提供者（一部、企業利用者を含む）を対象とした IoT セキュリティ対策の５指針を示す。IoT セキュリティ対策の５指針では、IoT のライフサイクル「方針」、「分析」、「設計」、「構築・接続」、「運用・保守」に沿って複数の要点を挙げ、要点ごとにポイントと解説、対策例を示す。なお、5 つの指針の内容については、「つながる世界の開発指針」（平成 28 年 3 月 独立行政法人情報処理推進機構）[6]を参考に、サービス提供者などへも対象者を広げ、より一般化したものである。

第 3 章においては、一般利用者向けの注意事項をルールとして記載する。

第 4 章においては、今後検討するべき事項を示す。

【参考】分野別セキュリティガイドラインへの展開例

報道関係者各位

平成 28 年 6 月 8 日
一般社団法人 重要生活機器連携セキュリティ協議会（CCDS）

CCDS、製品分野別セキュリティガイドライン第1版を策定

～IPA「つながる世界の開発指針」を車載・IoTゲートウェイ・金融端末・決裁端末の各分野に展開～

一般社団法人 重要生活機器連携セキュリティ協議会（会長：徳田 英幸 慶応義塾大学教授、代表理事：荻野 司 京都大学特任教授）は、今後の IT 社会において安全安心して利用できる IoT サービスの実現に不可欠な「セキュリティ・バイ・デザイン」の考え方を広く IoT 製品開発ベンダーに普及させることを目的に、車載・IoT ゲートウェイ・金融端末（ATM）・決裁端末（POS）の 4 分野の製品分野別セキュリティガイドライン第 1 版を策定いたしました。なお、この取組みは沖縄県「生活機器セキュリティ基盤形成促進事業」の補助を受けて実施しました。

今回策定した分野別セキュリティガイドラインは、昨年度、独立行政法人 情報処理推進機構（IPA）が策定した「つながる世界の開発指針※1」を基本的な考え方として参照し、製品分野ごとに対象となるシステム構成や対策すべき脅威（狙われるポイント）とリスク（被害）が異なることから、各分野の視点で取り組むべきセキュリティ対策についてとりまとめています。

分野別ガイドラインの主な内容：

- 対象とするシステム構成
- 想定されるセキュリティ上の脅威
- 製品ライフサイクルの各フェーズにおけるセキュリティの取組み
  （IPA「つながる世界の開発指針」との相関）
- 脅威分析・リスク評価の方法
- 製品全体およびセキュリティ対策機能の第三者セキュリティ評価

製品分野別セキュリティガイドラインは CCDS 公開資料サイト（以下の URL）をご参照ください。
https://www.ccds.or.jp/public_document/index.html

【参考】第13回 情報セキュリティEXPO アンケート結果

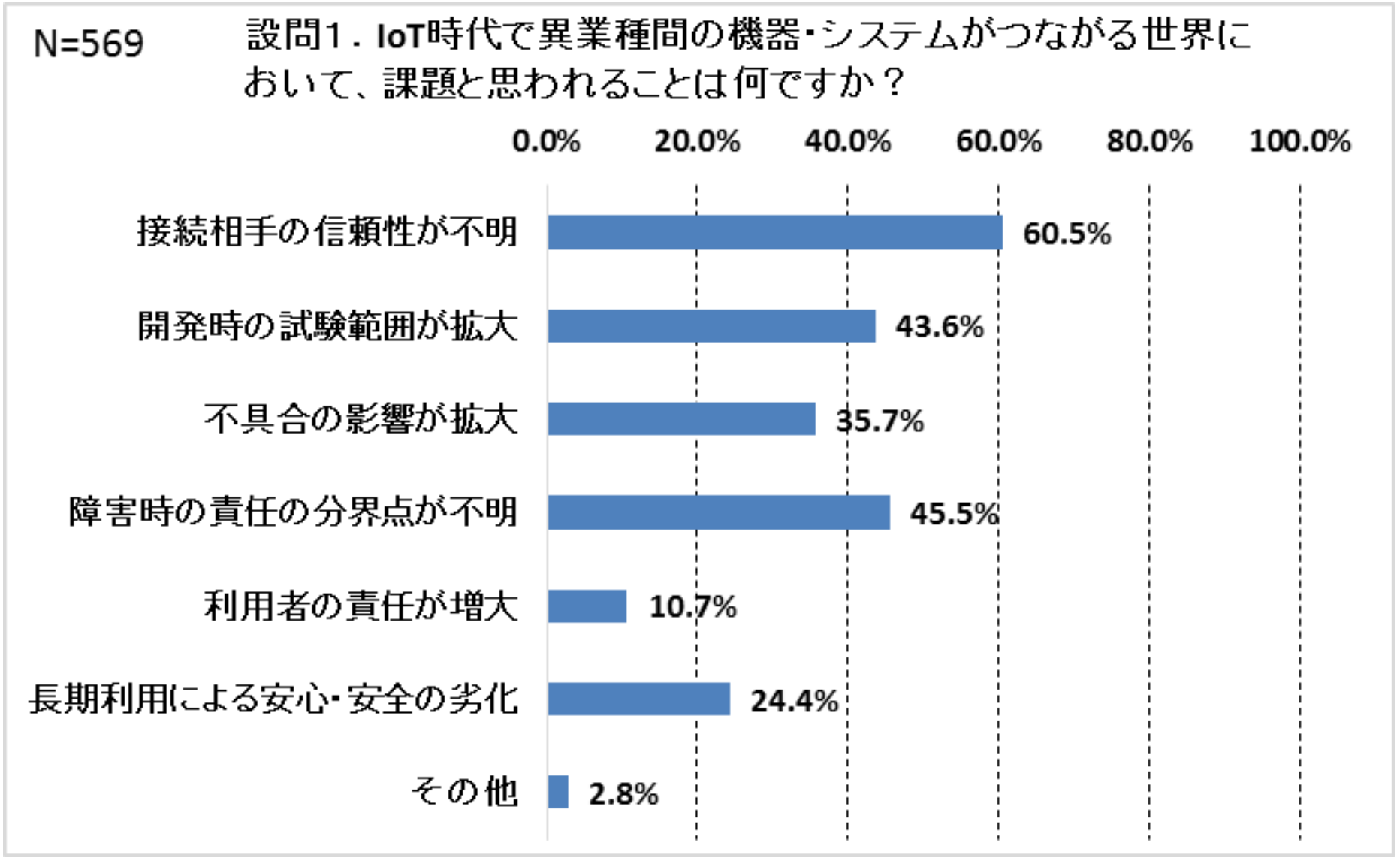
SEC Software Reliability Enhancement Center

2016年5月11日～13日に開催された第13回 情報セキュリティEXPOで「つながる世界の開発指針」の紹介のパネル展示を実施しました。
その場で、以下のアンケートを実施した結果を紹介します。

設問1：IoT時代の異業種間の機器・システムがつながる世界において課題と思われることは何ですか？

設問2：上記課題について、具体的に教えて下さい。また、その課題に対し、取り組んでいることがありましたら合わせて教えてください。

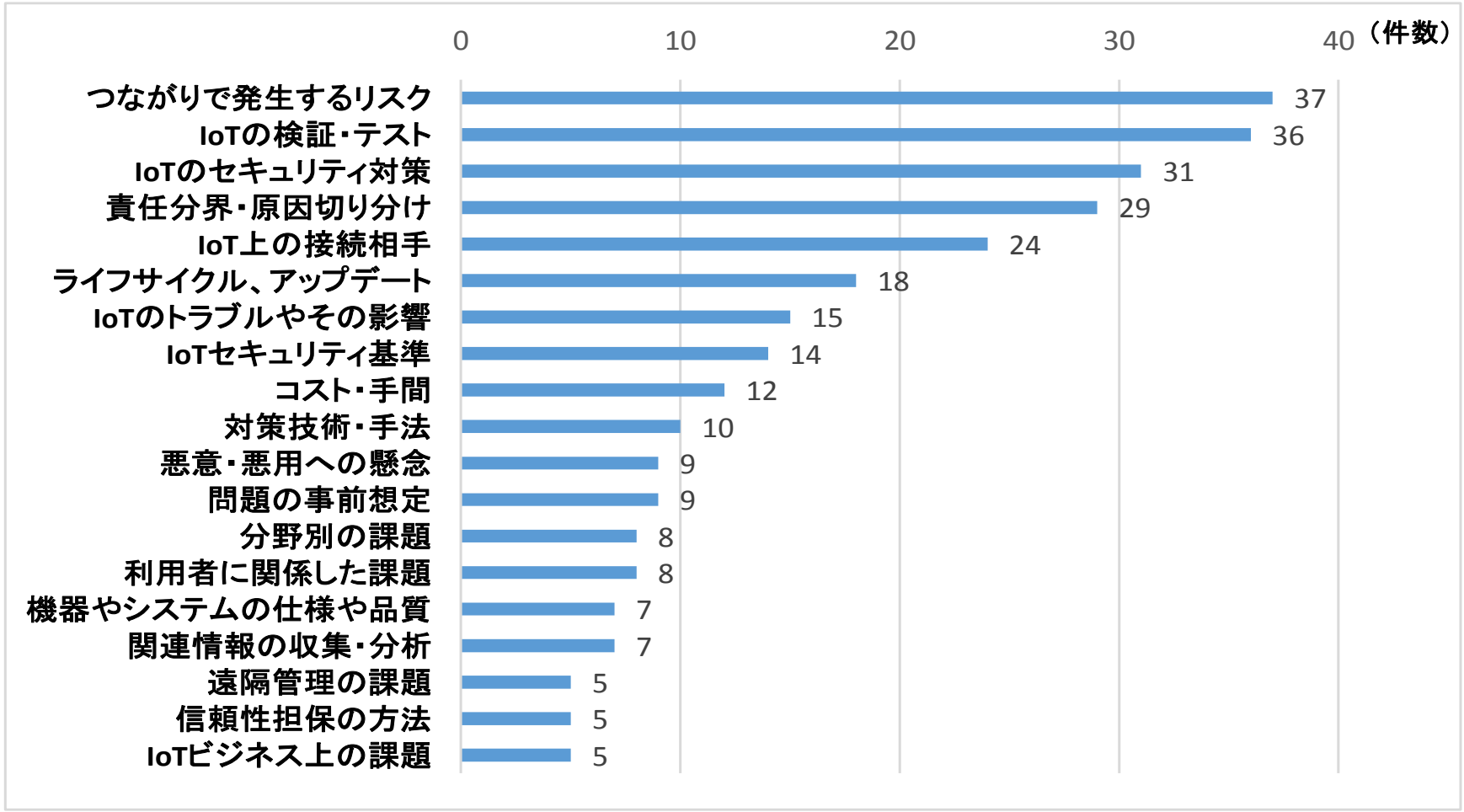
設問1. つながる世界の課題(グラフ)



設問2. 自由記述(分類に基づくグラフ)

SEC Software Reliability Enhancement Center

設問2. 上記課題について、具体的にお教えください。また、その課題に対し取り組んでいることがありましたら合わせてお教えください。



※SEC側で回答を分類(ひとつの回答に複数の分類に入れている場合あり)。

ご清聴ありがとうございました。