IPA Better Life with IT

「つながる世界の開発指針」
Part1: 基本となる考え方

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　遠山 真

Copyright © 2016 IPA, All rights reserved.

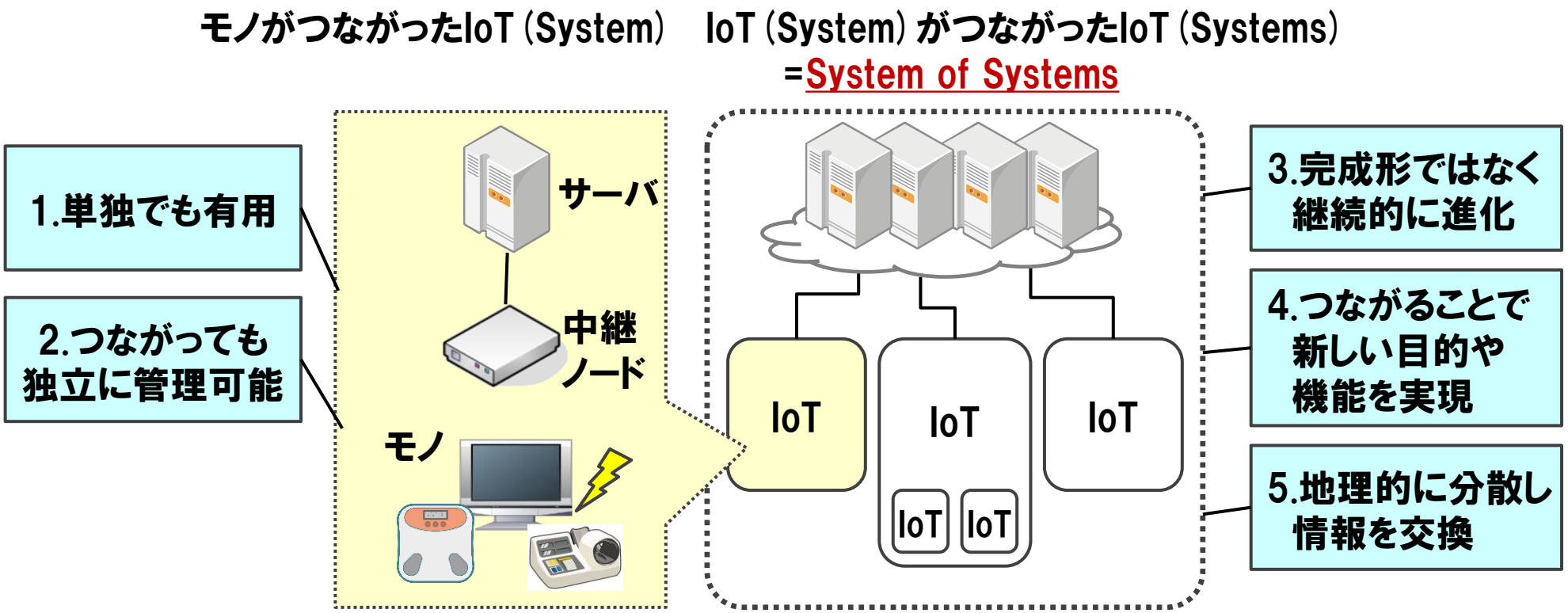
IPA Better Life with IT

「つながる世界」と「安全安心」の定義

Copyright © 2016 IPA, All rights reserved.

「つながる世界」とは

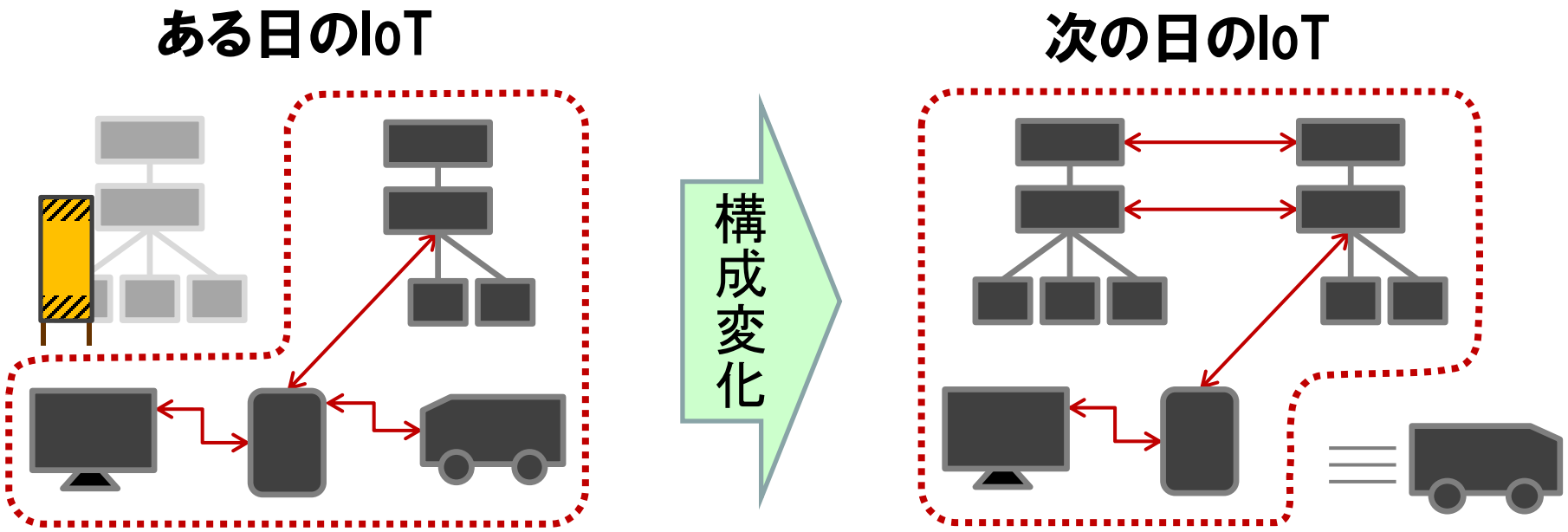
- 「つながる世界」≒ "IoT（Internet of Things）"
- かつ、"System of Systems"の性質を持つ前提
  - 独立に運用管理され単独でも有用なIoTが他のIoTとつながることにより進化し、より大きなIoTとして新たな目的や機能を実現



Copyright © 2016 IPA, All rights reserved.

つながる世界の特徴

- IoTの構成は日々変化（接続/分離、拡大/縮小、新旧混在）
  - アメーバのような変幻自在なシステム



- 構造も、リスクも、責任分界も、あいまいな部分が多い

Copyright © 2016 IPA, All rights reserved.

「安全安心」とは

SEC Software Reliability Enhancement Center

- IPAが「つながる世界」で実現したい対象の総称
  - 指針を簡潔に表現するために、用語を定義
  - いわゆる「安全」と「安心」ではない

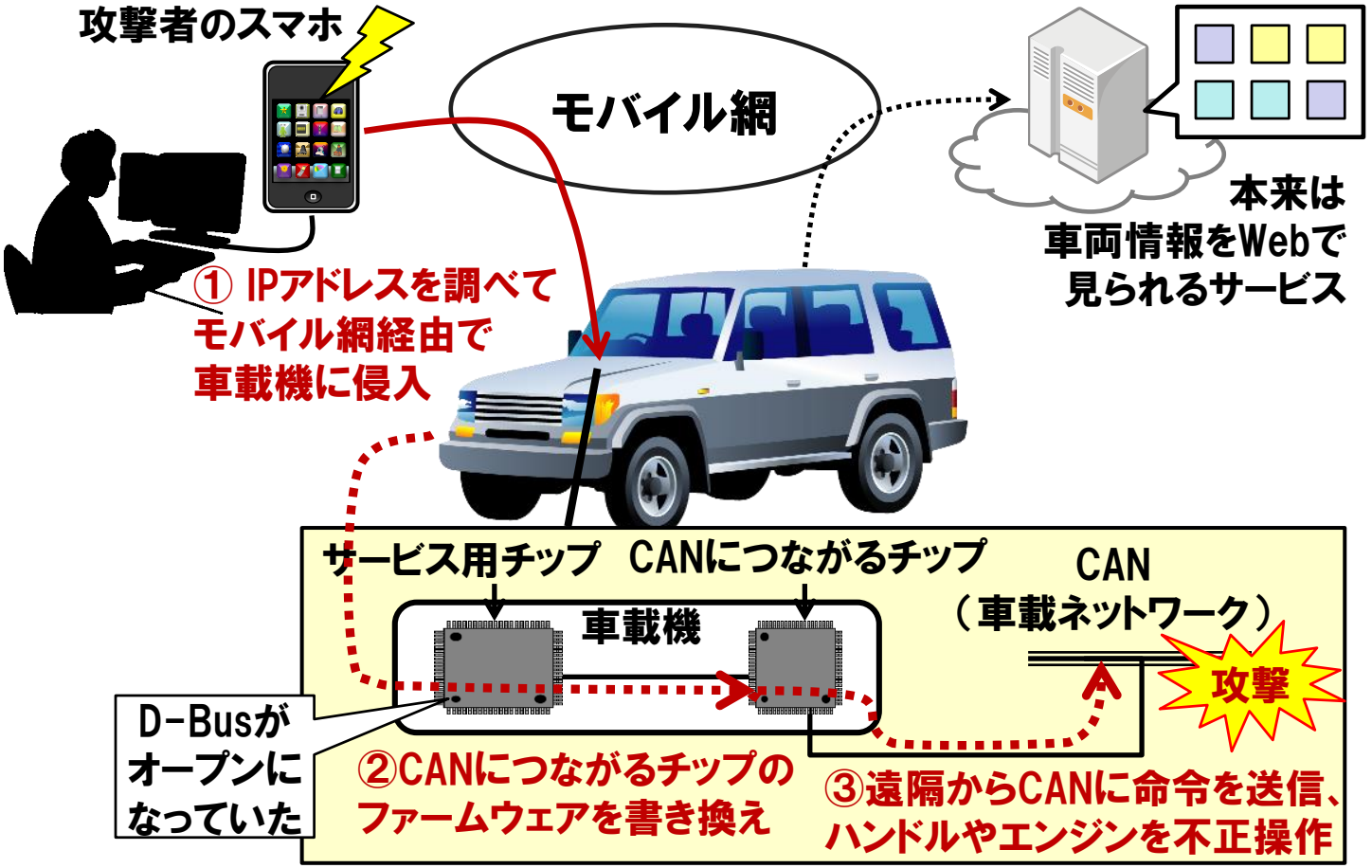
用語	本開発指針での意味
安全安心	対象とする機器やシステムのセーフティ、セキュリティ、リライアビリティが確保されていること。
セーフティ	機器やシステムが、人間の生活または環境に対する潜在的なリスクを緩和する度合い（リスク回避性）。
セキュリティ	人間または他の機器やシステムが、認められた権限の種類及び水準に応じたデータアクセスの度合いを持てるように、機器やシステムが情報及びデータを保護する度合い。
リライアビリティ	明示された時間帯で、明示された条件下に、機器やシステムが明示された機能を実行する度合い。加えて、他の機器やシステムと適切に情報を交換しつながること（相互運用性）、その他の機器やシステムに有害な影響を与えないこと（共存性）なども含む。

Copyright © 2016 IPA, All rights reserved.

セーフティとセキュリティの連携を重視

SEC Software Reliability Enhancement Center

- 近年のセーフティ機能は組込みソフトウェアや通信で実現
  - セーフティ機能をセキュリティ技術で守る
  - セーフティ設計とセキュリティ設計をすり合わせる　など



Copyright © 2016 IPA, All rights reserved.

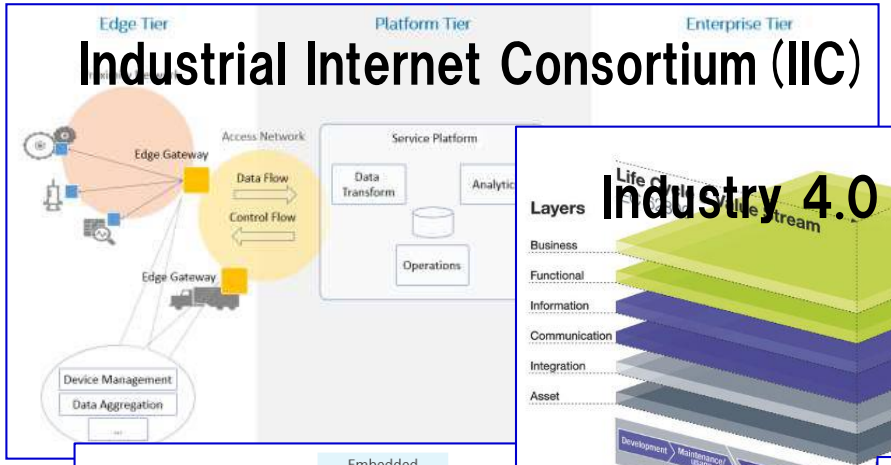
IPA Better Life with IT

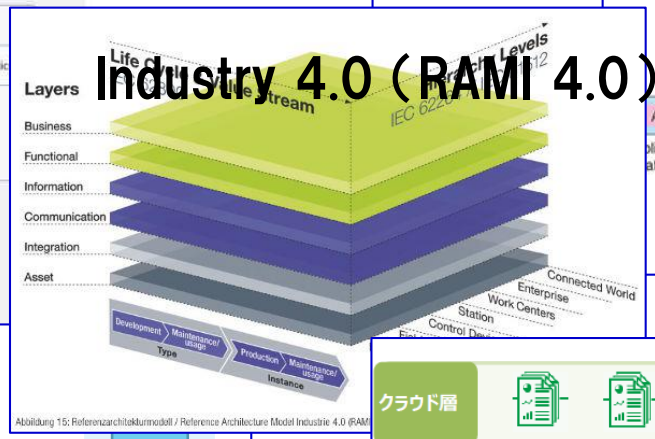
つながる世界の安全安心の考え方

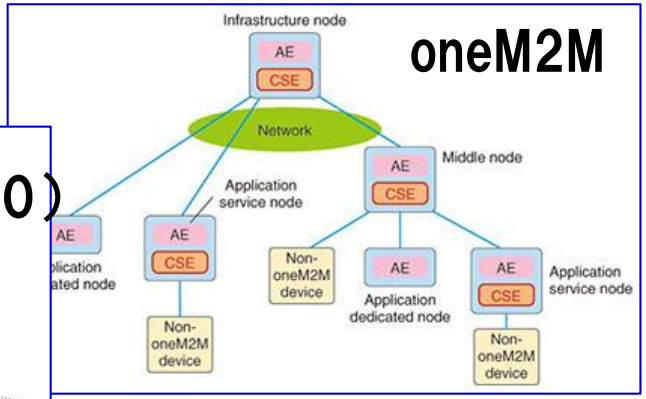
Copyright © 2016 IPA, All rights reserved.

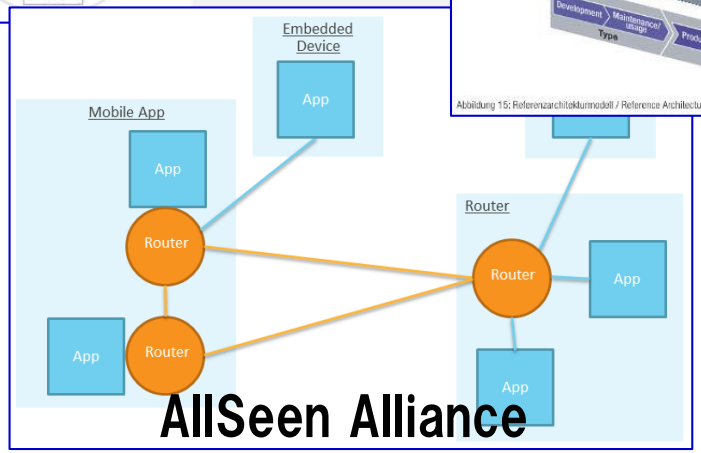
様々なIoTプラットフォームの登場

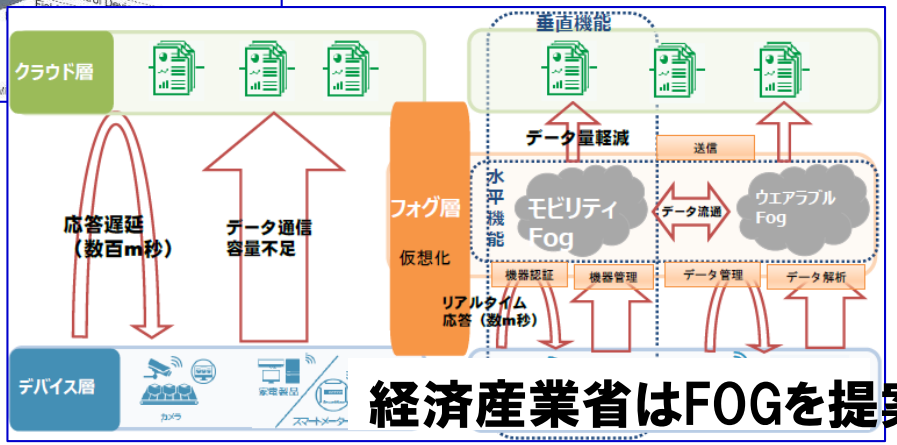
- 様々なIoT関連団体がIoTアーキテクチャを公表
- IT系大企業も、独自のIoTプラットフォームを構築・提供
- いずれも、安全安心を検討











Copyright © 2016 IPA, All rights reserved.

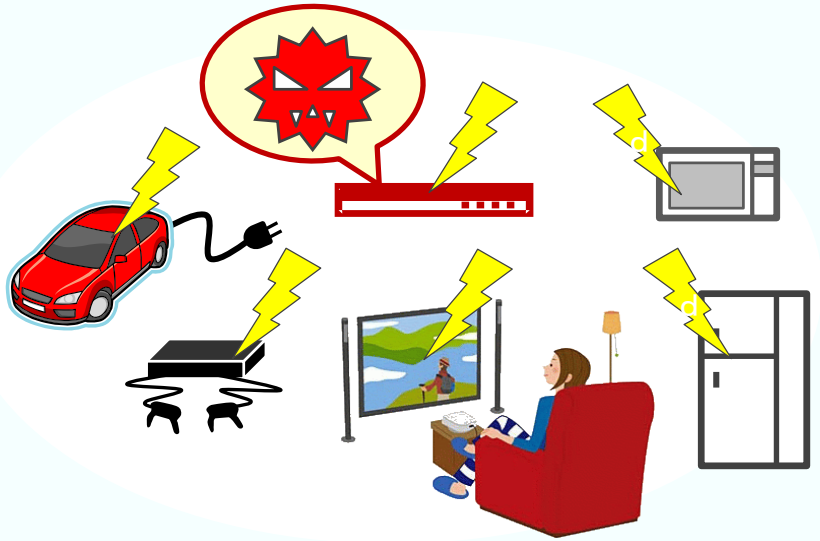
しかし、「モノ」のつながり方は多様

SEC Software Reliability Enhancement Center

- モノ（自動車、家電、他）の利用者（企業や消費者）がIoTプラットフォームにつなげるとは限らない

ベンチャー企業が
モノとインターネットを組み合わせて
IoTサービスを構築

消費者が家庭内LANに
多様な生活機器を接続



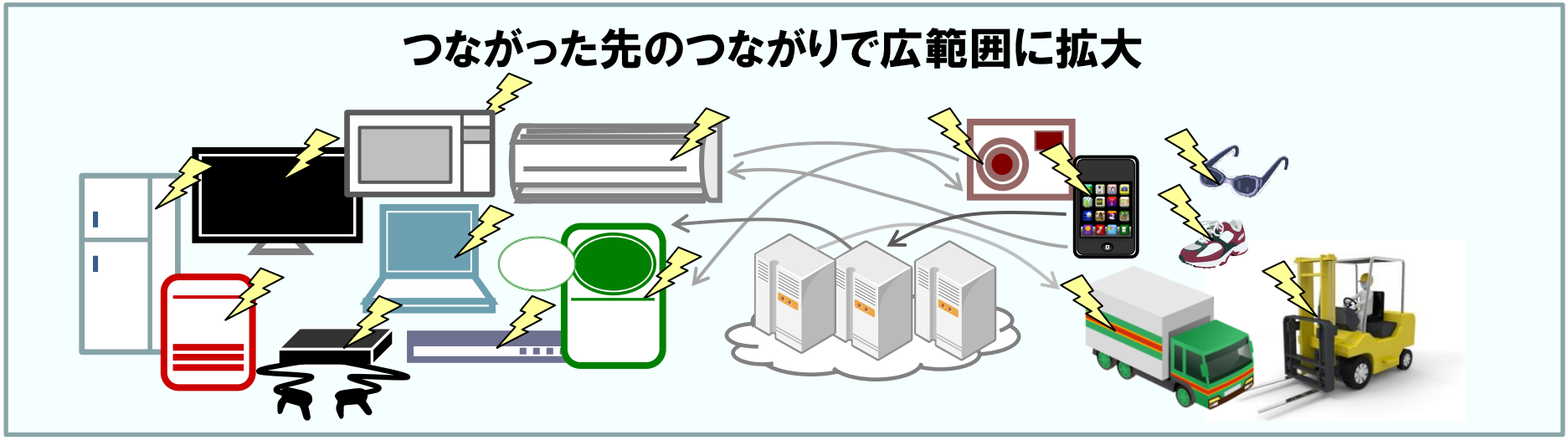
- 上図の場合、つながることによるリスクが高まる可能性あり

Copyright © 2016 IPA, All rights reserved.

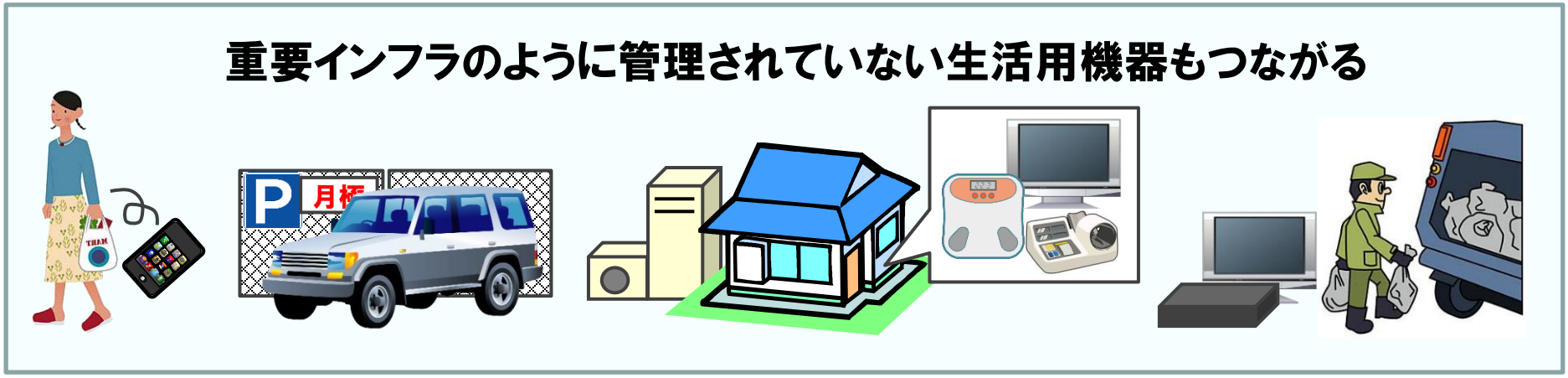
つながることによるリスク例（その1）

SEC Software Reliability Enhancement Center

- 1）想定しないつながりが発生する



- 2）管理されていないモノもつながる



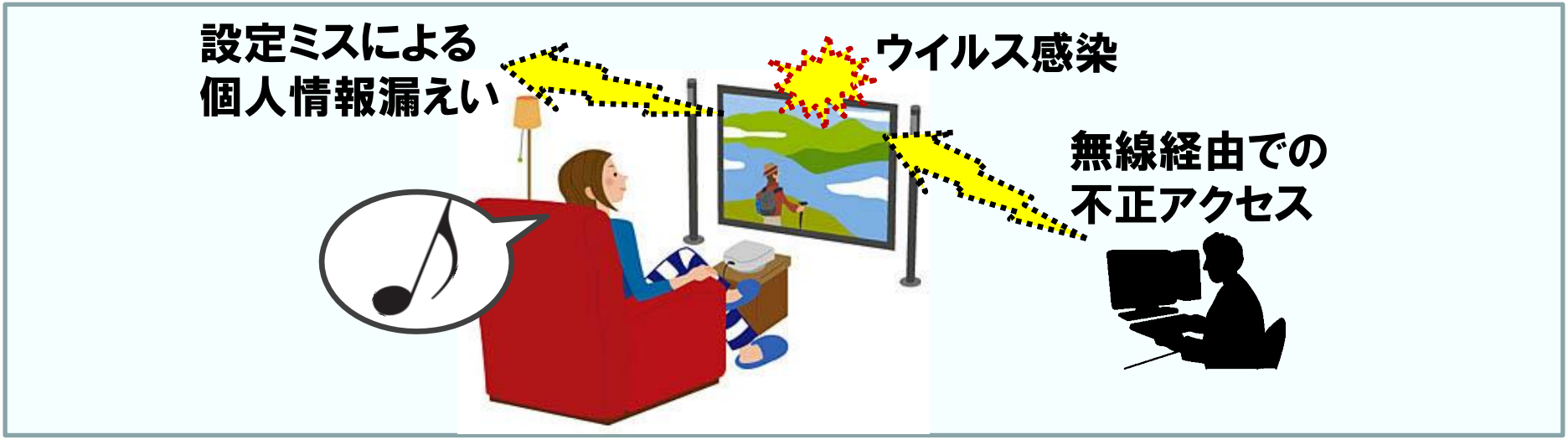
Copyright © 2016 IPA, All rights reserved.

つながることによるリスク例（その2）

SEC Software Reliability Enhancement Center

- 3）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

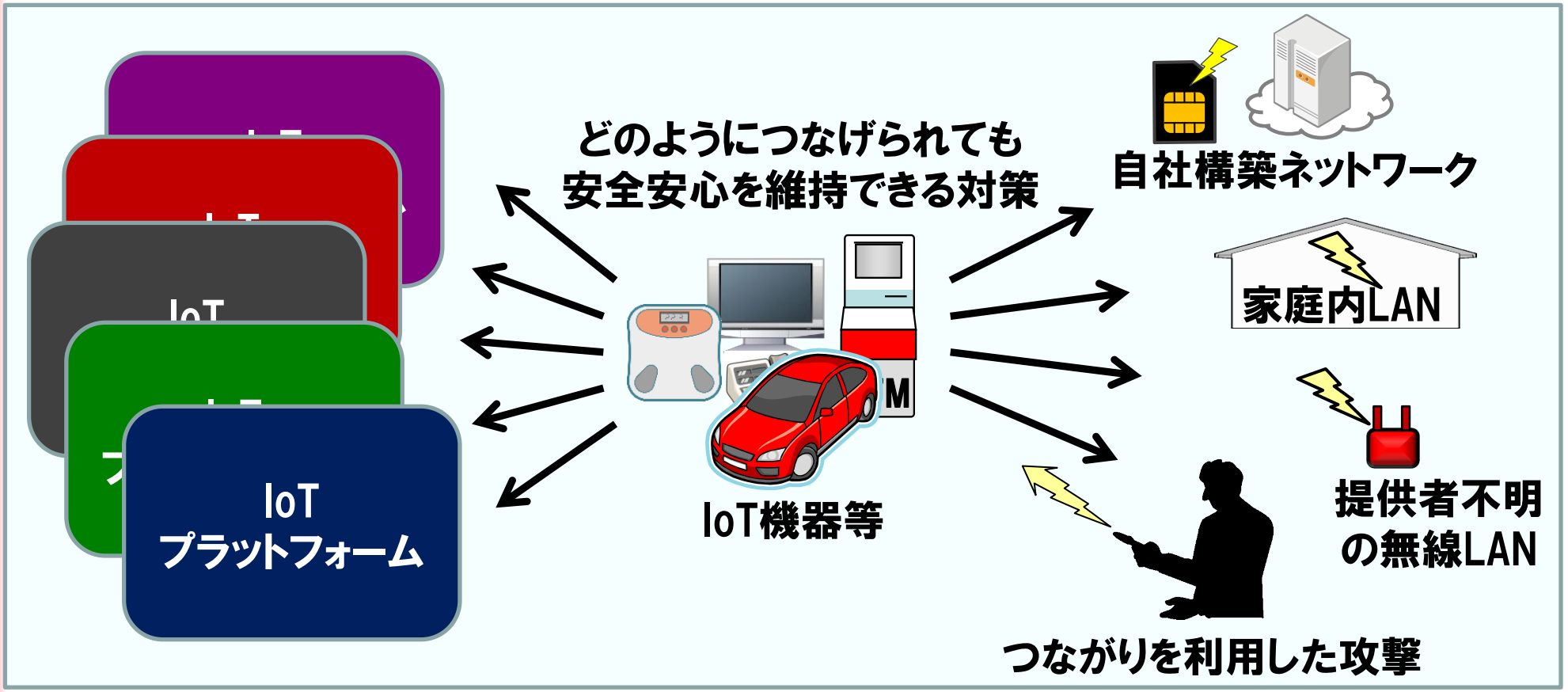
- 4）問題が発生しても ユーザにはわかりにくい



Copyright © 2016 IPA, All rights reserved.

そこで、「モノ」の安全安心対策

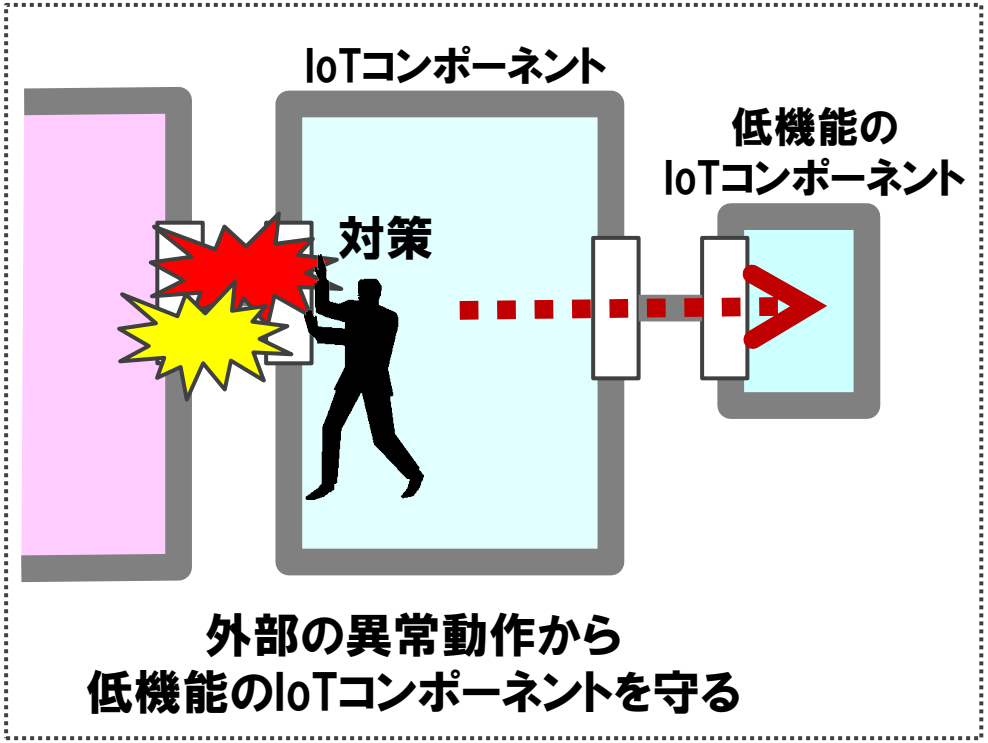
- どのようにつなげられても安全安心を維持できる「モノ」へ
  - つながりを経由した攻撃や異常信号などに対応
  - 自分に異常が発生しても、つながる先に迷惑をかけない　など



Copyright © 2016 IPA, All rights reserved.

IoTコンポーネントの安全安心対策の例

- 上位のコンポーネントが低機能のIoTコンポーネントを守る
- 自分に異常が発生しても、つながる先に迷惑をかけない

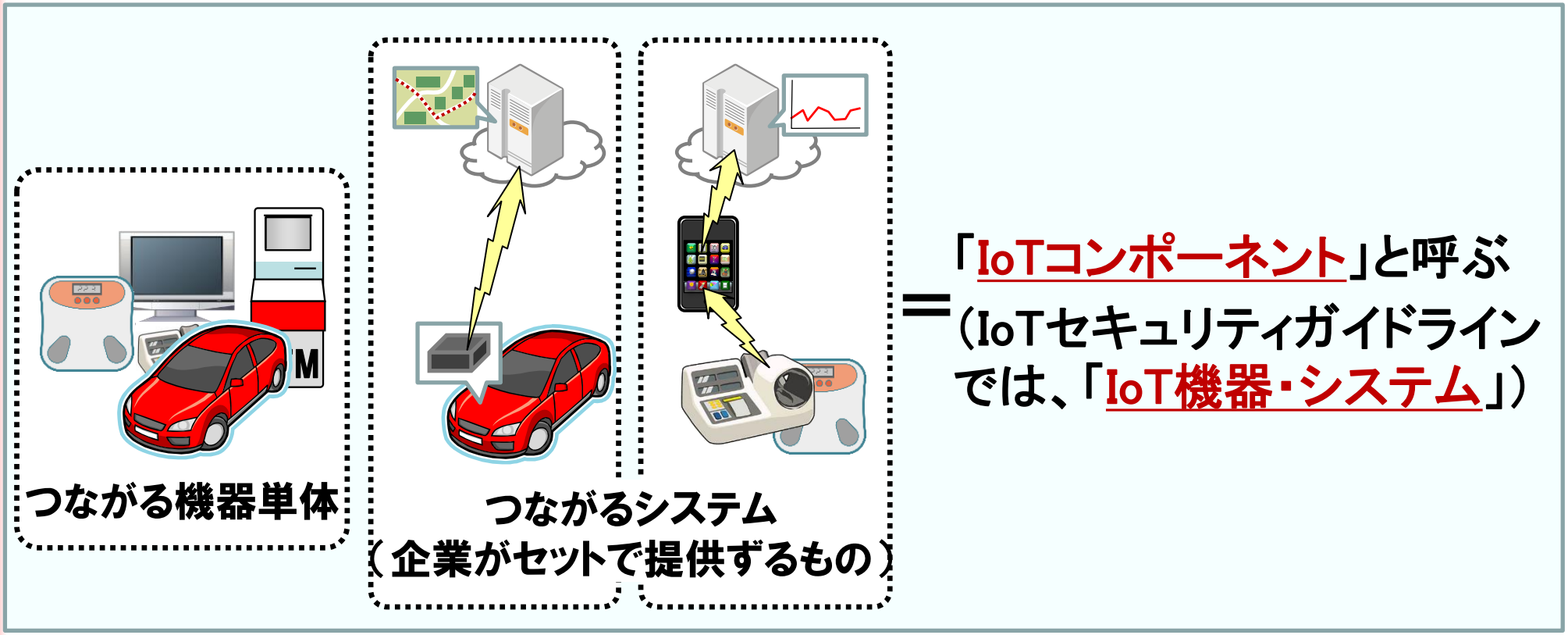


Copyright © 2016 IPA, All rights reserved.

安全安心対策の最小単位（IoTコンポーネント）

SEC Software Reliability Enhancement Center

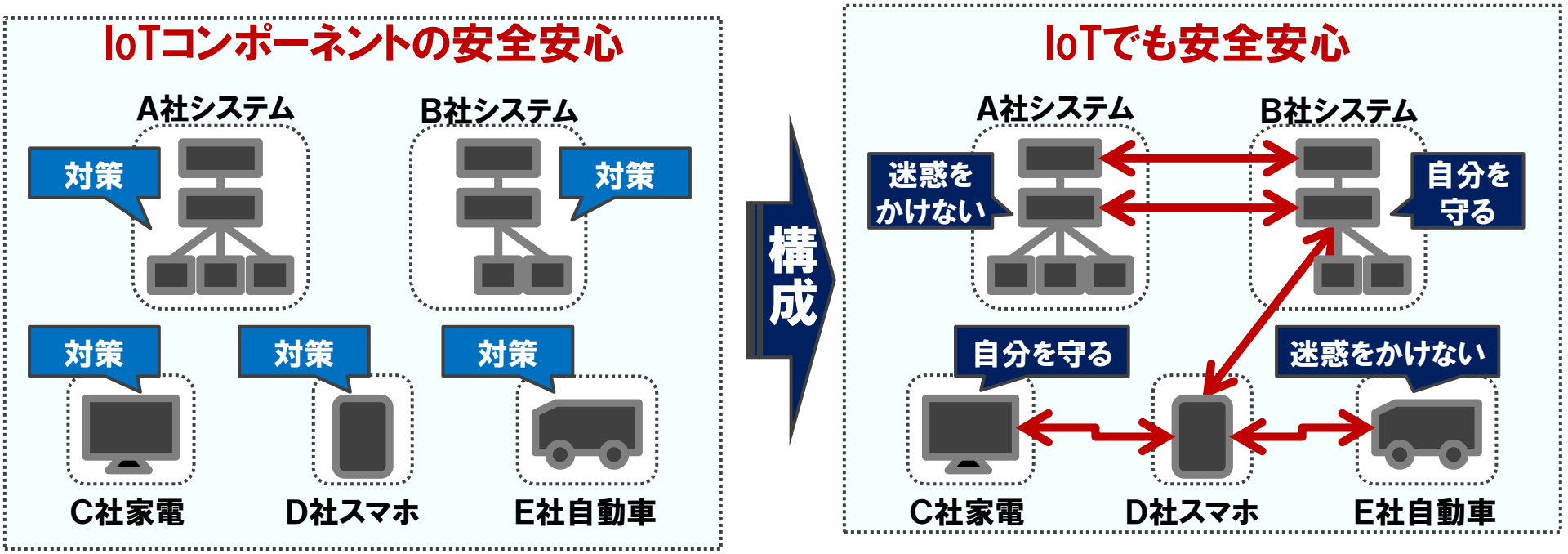
- 企業が単体またはセットで提供するモノ（機器やシステム）は、その企業が安全安心対策を行うものと想定
  - 機器単体の例：自動車、ヘルスケア機器、家電など
  - システム例：身体データをサーバで分析する健康サービスなど



Copyright © 2016 IPA, All rights reserved.

IoTコンポーネントの安全安心→IoTでも安全安心

- 構成要素が安全安心であれば、IoTの中でも安全安心
  - IoT同士で構成されるIoTも同様（"System of Systems"）



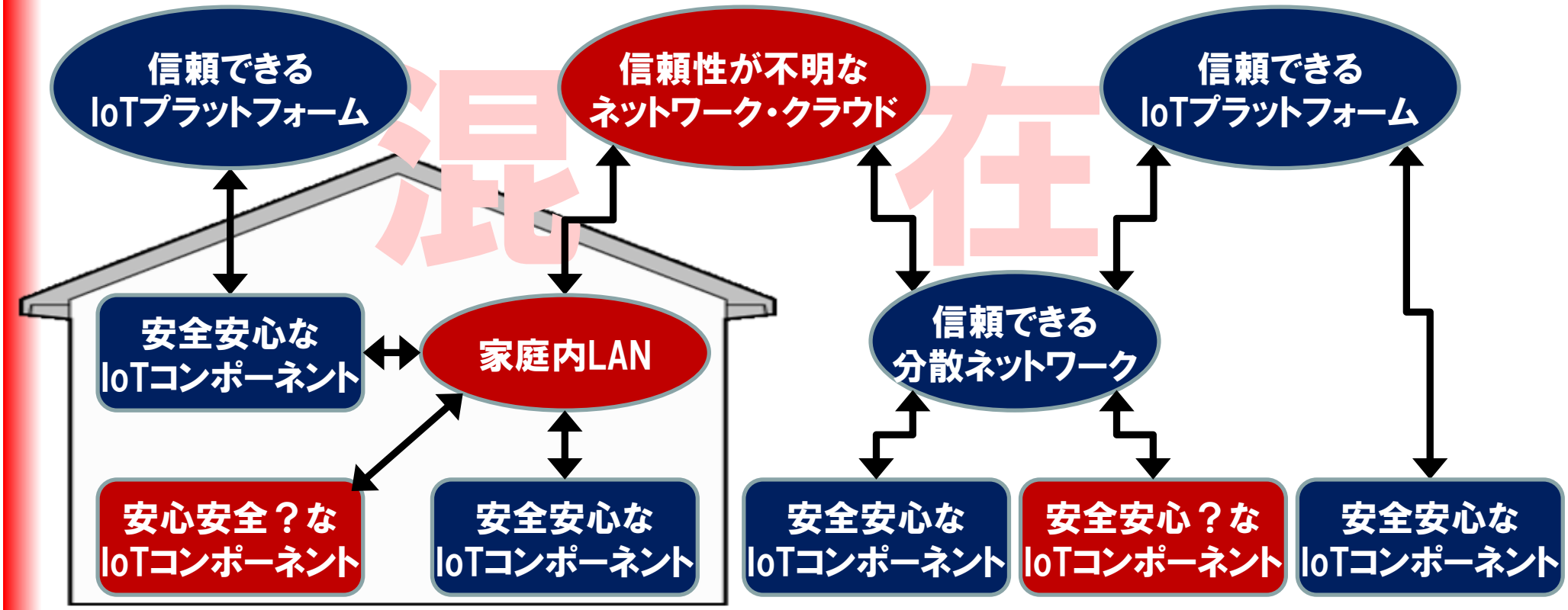
- ただし、IoT全体が安全安心になるわけではない

Copyright © 2016 IPA, All rights reserved.

将来も、IoTには「安全安心」と「不安」が混在

SEC Software Reliability Enhancement Center

- IoTには、安全安心が不明なモノも混在
  - 安全安心対策が不十分なネットワーク・クラウド
  - 消費者が自作したり個人輸入した機器など
- IoT全体については、IoT推進コンソーシアムで検討



Copyright © 2016 IPA, All rights reserved.

IPA Better Life with IT

IoTコンポーネントの安全安心の検討プロセス

Copyright © 2016 IPA, All rights reserved.

1）IoTコンポーネントの守るべきものの整理

SEC Software Reliability Enhancement Center

- 冷蔵庫なら「冷やす」といった本来機能と、「モノ」がネットワークにつながるためのIoT機能を分けて考えた

要求に応じて
利用可能であること

IoTアプリ、通信機能、
セキュリティ対策のための
機能など

機器やシステム本来の機能、
セーフティ対策のための
機能など

個人情報、決済情報、
センサーデータなど

自動販売機内の商品、
ATM内の現金、
本体や部品など

IoT機能
（通信、連携、集約等）

本来機能
（サーバ、GW、
モノ等の機能）

情報

その他

Copyright © 2016 IPA, All rights reserved.

2）つながり方のパターンの整理

SEC Software Reliability Enhancement Center

- IoTコンポーネントのつながり方のパターンを整理

つなげた者

【メーカーや関連会社がつなげるケース】

メーカーが設計時に想定しているケース

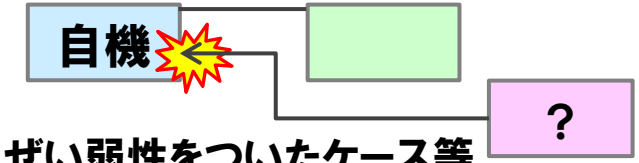
【サービス事業者がつなげるケース】

メーカーが設計時に想定していないケース

【ユーザがつなげるケース】

意図的だけでなく、誤ってつなげるケースも

【攻撃者がつなげるケース】



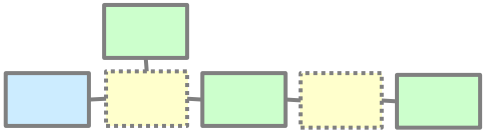
ぜい弱性をついたケース等

つながりの形

【直接的】

【固定的】

【複合的】



【間接的】

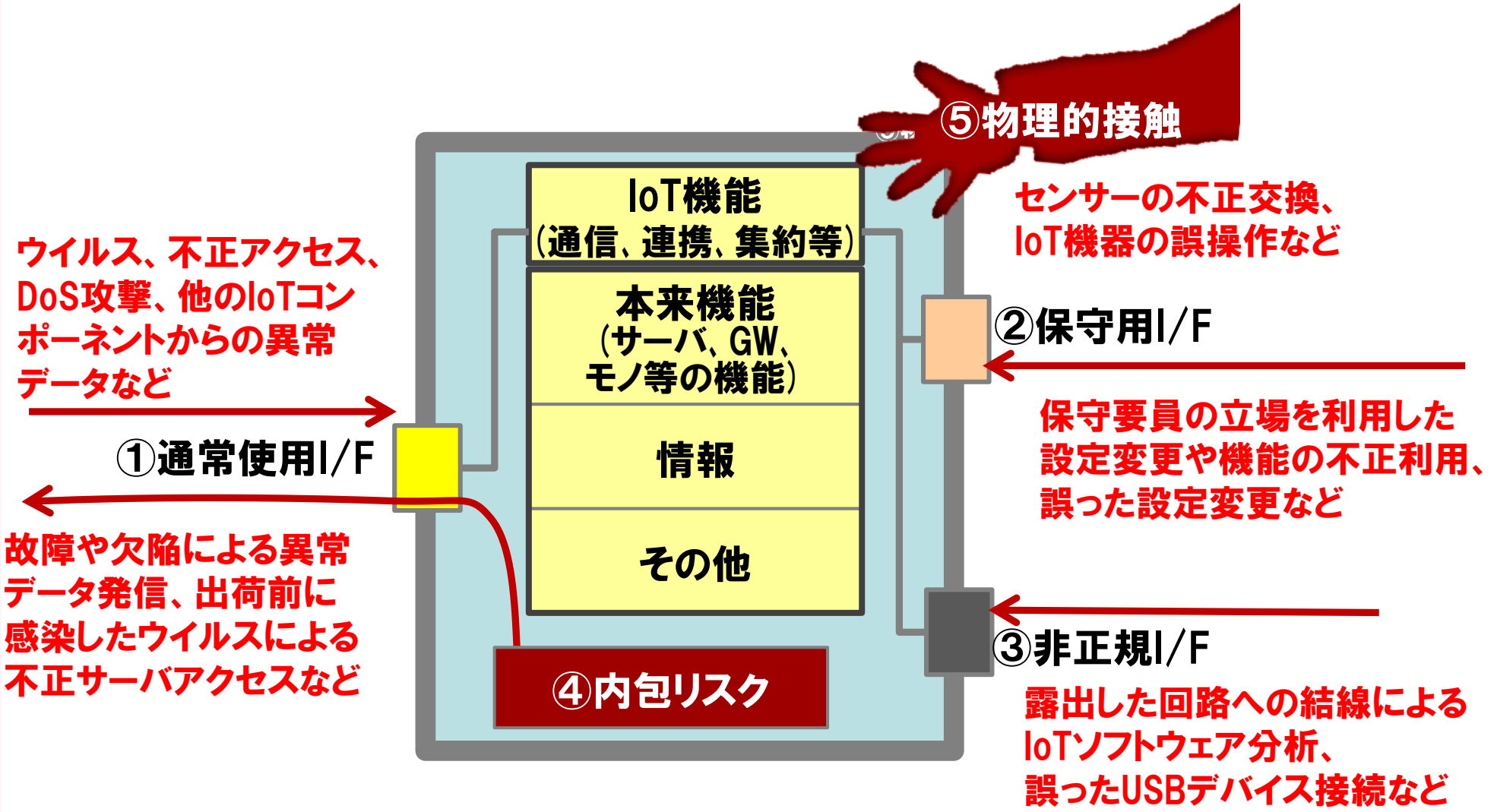
【動的（必要時に接続）】

Copyright © 2016 IPA, All rights reserved.

3）IoTコンポーネントのリスク箇所の整理

SEC Software Reliability Enhancement Center

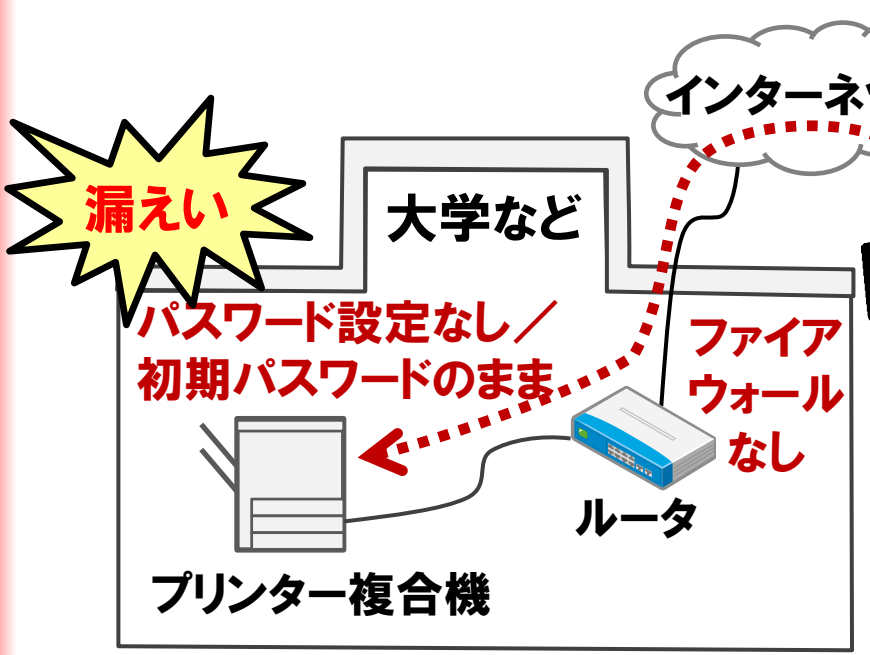
- リスク箇所（リスクの入口となりそうな箇所）を整理



Copyright © 2016 IPA, All rights reserved.

4）各パターンにおけるリスクの想定

- 既存のリスク事例の収集及び将来のリスクの想定
  - 事例1）複合機の蓄積データがインターネットで公開状態
    - パスワードが未設定、ファイアウォールがなかった
  - 事例2）スマホ経由で自動車の操作乗っ取りが可能に
    - そのような攻撃を想定しておらず、対策が取られていなかった



複合機の蓄積データが参照可能

遠隔から自動車を不正操作

Copyright © 2016 IPA, All rights reserved.

5)リスク分析及び開発指針の導出

- リスク分析表の作成
  - 「守るべきもの」や「つながりのパターン」との関係を整理、分析
- 分析結果から開発指針を導出

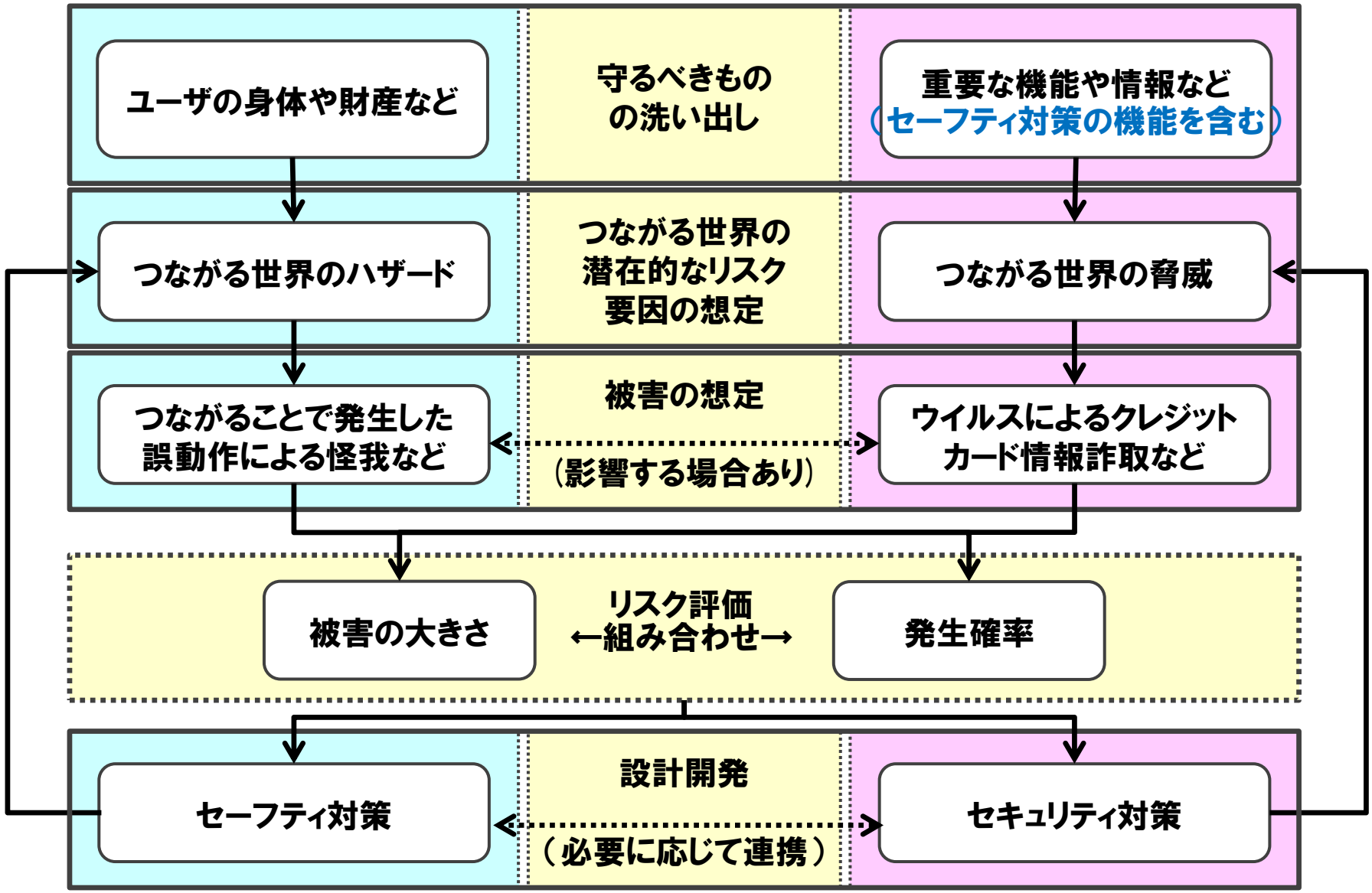
WHAT		WHO						HOW					WHOM					WHERE					WHEN				WHY	
何が起きたか		誰がつなげたか						どのようにつなげたか					何が危害を受けたか					どこで発生したか					どの段階で発生したか				なぜ発生したか	
機器種別	リスク例	メーカーや関連企業	サービス事業者	ユーザ（意図的）	ユーザ（誤接続）	攻撃者	偶発的	直接的	間接的	固定的	動的	複合的	IoT機能	本来機能	データ	身体や財産	その他	通常使用I／F	メンテナンス用I／F	非正規I／F	内包	物理的接触	企画・設計・開発	製造・出荷	運用（供給側）	運用（ユーザ側）	廃棄・リサイクル	主要な原因	IoTに着目した課題/問題
プリンター複合機	インターネットに接続することを想定していないプリンター複合機の蓄積データが公開状態に。初期パスワードも文書で公開。	○								○					○				○							○		インターネット接続の想定不足	ファイアウォールに守られたクローズドな環境への設置を想定していた。
																												初期パスワードの変更依頼不足	
																												初期パスワードを記載した文書の公開	
ATM	物理鍵を不正に入手しATMの保守用扉を開けてウイルスを感染させるとともに、さらに電話機等を取り付け、その電話機等にメールを送ることで現金引き出した。					○		○			○					○（現金）			○			○				○		攻撃事例の把握、共有不足	攻撃者に保守用扉を開けられたり、保守用USB端子に電話機等をつなげられるリスクの想定が不十分であった。
																												保守用扉のアクセス管理不足	
																												保守用インタフェースの開放	
																												ATM端末のウイルス感染	
IoT全般	〔想定事例〕IoT同士がつながるうちに、想定されたないIoTまでつながり、情報が漏えいした。						○								○			○						○				個々のIoTの管理不足	意図しないつながりにおいても、安全安心を維持する必要がある。
																												つながりの全体像を把握する機能なし	
IoT機器	〔想定事例〕拾ったIoT機器をいじっていたら遠隔機能が動作し、ユーザの財産に損害を与えた。				○						○			○		○		○							○			ユーザ認証機能の不足	拾得者などによる意図しない利用に対しても、安全安心を考える必要がある。
																												不自然な操作に対する確認の不足	
自動車	ローンが滞ったユーザの自動車を遠隔からロックしたり、ホーンをならすサービスが元従業員に不正利用。		○							○				○				○							○			アカウントの管理不足	内部犯行を想定していなかった。
																												異常な利用を防ぐ仕組みの不足	
車載器	モバイル網経由で車載器にアクセス、チップのファームウェアを書き換え、車載ネットワークに制御命令を送信、自動車のハンドルやブレーキを遠隔制御。	○				○			○		○			○					○	○						○			モバイル網のアクセス管理不足	・守るべきものが守られていなかった。 ・セキュリティの問題がセーフティに与える影響の想定が不十分であった。 ・遠隔アップデート機能のセキュリティが不十分であった。
																												スマホ－車載器間通信の非保護	
																												車載器権限の認証なし	
																												アップデートファイルの暗号化なし	
																												自動車制御系へのアクセス管理不足	
IoT機器	工場の検査時にウイルス感染、出荷され、IoT接続された際に感染が広がった。			○				○									○（製品）				○			○				工場でのセキュリティ検査不足	つながる相手に影響を与えないという配慮が不足していた。
																												ウイルスチェック機能なし	
																												異常時の自律制御機能なし	
IoT機器	〔想定事例〕廃棄・リサイクルされた機器をつなげたら、前の所有者のIoT設定が残っていてサーバにつながってしまった。				○					○	○						○	○									○	廃棄・リサイクル時の設定消去なし	廃棄・リサイクル時の対策を検討する必要がある。
IoT全般	〔想定事例〕災害時に、災害対策用のIoTが一斉に立ち上がり、無線が輻輳、IoTが使用できなくなった。						○				○	○	○	○				○						○				社会全体としてのIoTの把握不足	周囲及び自己の現在の状態を把握し、対応する必要がある。
POS	センターサーバに不正アクセス、POS端末にウイルスを感染させ、顧客の決済情報を不正に収集。		○			○			○	○					○			○							○			攻撃事例の把握、共有不足	自社に関連する機器への攻撃が増大していたのに、対策していなかった。
																												センターサーバのアクセス管理不足	
																												POS端末のウイルス感染	
家電	〔想定事例〕ユーザが家庭用の家電操作機器の通信を中継・延長し、遠隔から家電を操作したところ家族が事故にあった。			○						○						○		○								○		ユーザのリスク認識不足	ユーザがつながる世界のリスクを認知させる必要がある。

※本表については、開発指針の付録を参照

対象の方向性 ＼ 対象読者	対策されるべき課題		
	経営者	開発者	保守者
つながりによるリスクを想定する	基本方針が策定されていない。	リスクが想定されていない。	
物理的なリスクを認識する		リスクが想定されていない。	
知らない相手でも安全安心につながられる設計をする		意図しない使われ方やつながりを考慮できていない。	
内部不正や情報漏えいに備える	社員のモラルや訓練、リスク想定が不足している。		
安全安心の設計の整合性を確認する		双方の技術者が連携できていない。	
個々でも全体でも守れる設計をする		IoTとしての守るべきものと守り方が明確でない。	
時間が経っても安全安心を維持する		アップデート機能の安全性が不足している。	アップデート機能の不正利用を防げない。
つながる相手に迷惑かけない設計をする		自身の問題の他への波及を止められない。	自身の問題の他への波及を止められない。
廃棄・リサイクル時の機密漏えいに備える		廃棄・リサイクル時の機密漏えい対策が不十分。	廃棄・リサイクル時の機密漏えい対策が不十分。
自身がどのような状態かを把握・記録する	緊急対応体制が整備できていない。	自身の問題を検知できない。	自身の問題を検知できない。
最新のIoTリスクを把握・情報共有する			最新のリスクを把握できていない。
ユーザにつながることによるリスクを知ってもらう			ユーザがつながるリスクを防げない。

Copyright © 2016 IPA, All rights reserved.

リスク対策のフロー



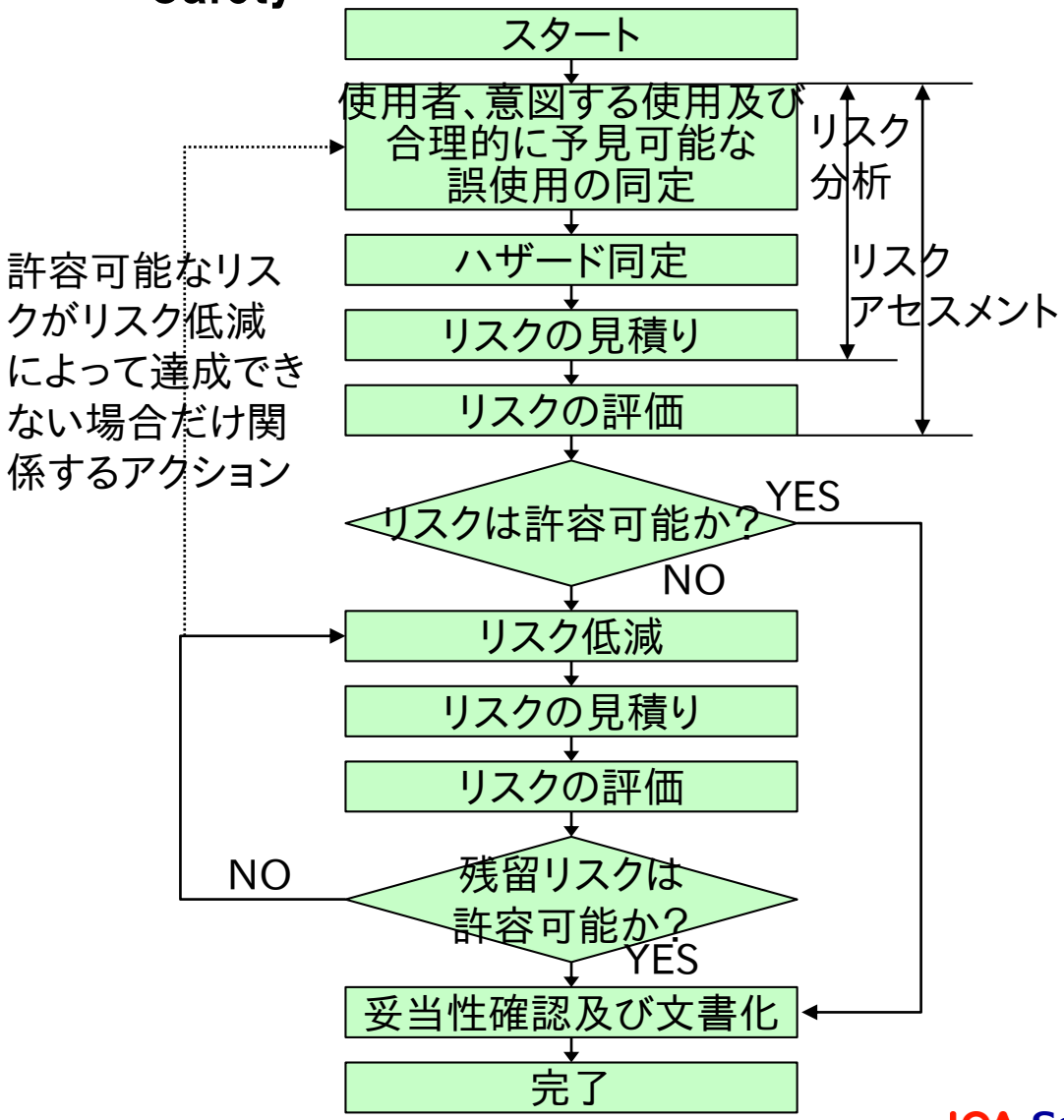
Copyright © 2016 IPA, All rights reserved.

国際標準におけるリスク評価プロセス

SEC Software Reliability Enhancement Center

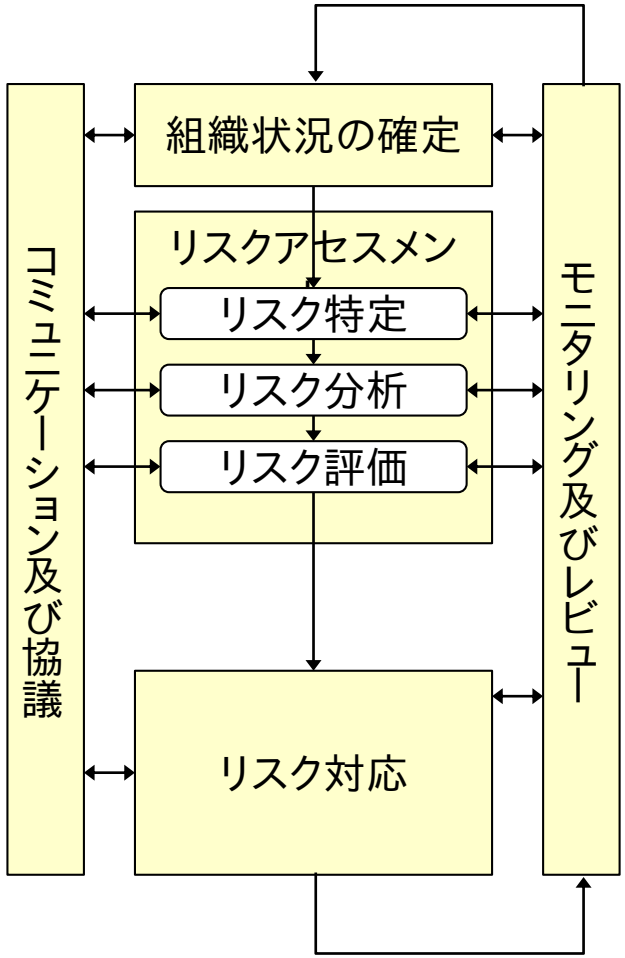
Safety

ISO/IEC Guide 51のリスクアセスメントとリスク低減プロセス



Security

ISO 31000のリスクマネジメントプロセス



Copyright © 2016 IPA, All rights reserved.