IPA Better Life with IT

IoTと日本を取りまく現状

独立行政法人 情報処理推進機構
技術本部 ソフトウェア高信頼化センター 調査役
工学博士 田丸喜一郎

Copyright © 2016 IPA, All Rights Reserved

SEC Software Reliability Enhancement Center

Internet of Things

an infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react.

物理世界と仮想世界の情報を処理し、それらが相互作用できるように
物・人・システム・情報資源をインテリジェントサービスにより
相互接続するインフラ

[SOURCE: ISO/IEC JTC 1/SWG 5&ISO/IEC 24760-1:2011, 3.1.1]

Copyright © 2016 IPA, All Rights Reserved

“That 'Internet of Things' Thing” by Kevin Ashton

SEC Software Reliability Enhancement Center

- Jun 22, 2009- 1 could be wrong, but I’m fairly sure the phrase ’Internet of Things’ started life as the title of a presentation I made at Procter and Gamble (P&G) In 1999. Linking the new Idea of RFID In P&G's supply chain to the then-red-hot topic of the Internet was more than just a good way to get executive attention. It summed up an important insight-one that 10 years later, after the Internet of Things has become the title of everything from an article in Scientific American to the name of a European Union conference. Is still often misunderstood.
- The fact that I was probably the first person to say "Internet of Things" doesn't give me any right to control how others use the phrase. But what l meant, and still mean, is this: Today computers-and, therefore, the Internet- are almost wholly dependent on human beings for information. Nearly all of the roughly 50 petabytes (a petabyte is 1,024 terabytes) of data available on the Internet were first captured and created by human beings-by typing, pressing a record button, taking a digital picture or scanning a bar code. Conventional diagrams of the Internet include servers and routers and so on, but they leave out the most numerous and important routers of all: people. The problem is, people have limited time, attention and accuracy-all of which means they are not very good at capturing data about things in the real world.
- And that's a big deal. we're physical, and so is our environment. Our economy, society and survival aren't based on ideas or information-they're based on things. You can't eat bits, burn them to stay warm or put them in your gas tank. Ideas and information are important, but things matter much more. Yet today's information technology is so dependent on data originated by people that our computers know more about ideas than things.
- If we had computers that knew everything there was to know about things-using data they gathered without any help from us-we would be able to track and count everything, and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling, and whether they-refresh or past their best.
- We need to empower computers with their own means of gathering information, so they can see, hear and smell the world for themselves. In all Its random glory. RFID and sensor technology enable computers to observe. Identify and understand the world-without the limitations of human-entered data.
- Ten years on, we’ve made a lot of progress. But we in the RFID community need to understand what's so Important about what our technology does, and keep advocating for it. It's not just “bar code on steroids" or a way to speed up toll roads, and we must never allow our vision to shrink to that stale. The internet of Things has the potential to change the world, just as the Internet did. Maybe even more so.

出展：RFID Journal Jun 22,2009

Copyright © 2016 IPA, All Rights Reserved

国際電気通信連合（ITU）150周年賞受賞者（2015年5月）

SEC Software Reliability Enhancement Center

- ビル・ゲイツ（60歳）米国
  - マイクロソフト社の共同創業者兼元会長兼顧問、ビル& メリンダ・ゲイツ財団の共同会長など役職多数。
  - パソコンを通じたインターネットへのアクセスの普及に 多大な貢献。
- ロバート・E・カーン（76歳）米国
  - CNRI 理事長。AT&T やベル研究所、MIT 電子工学部、国防 高等研究計画局等を歴任。
  - アーパネット（インターネットの原型）を提唱し、イン ターネットの基盤となる TCP/IP を開発。
- トーマス・ウィーガンド（45歳）ドイツ
  - ベルリン技術大学電子工学コンピュータ科学部教授。
  - ITU電気通信標準化部門やISO/IEC等の標準化団体の会議 に参画し、MPEG 等の映像データの圧縮方式の標準化に尽力。
- マーク・I・クリボシェフ（82歳）ロシア
  - モスクワ電気通信研究所の博士、ロシア連邦科学技術学会の通信委員等を歴任。
  - 高精細のテレビ映像の国際間の交換が可能になるよう標準化に尽力。
- マーティン・クーパー（86歳）米国
  - Dyna LLC の会長や国立エンジニアリング学会のメンバー など役職多数。
  - モトローラ在職中の 1973 年に世界初のポータブル携帯電話を開発するなど、無線通信産業のパイオニア。
- 坂村 健（63歳）日本
  - 東京大学大学院情報学環教授、YRP ユビキタス・ネットワ ーキング研究所の所長など役職多数。
  - ユビキタスネットワークや IoT（Internet of Things）の 起源となったオープンアーキテクチャ TRON を提唱。

（参考1）国際電気通信連合（ITU: International Telecommunication Union）

1865年創設（今年は150周年）。電気通信に関する国連の専門機関で、国際的な周波数の分配、電気通信の標準化及び開発途上国に対する支援が主要な業務。本部はスイス（ジュネーブ）。日本を含む193か国が加盟。

日本は1959年以来、理事国に連続して選出。米国と並び最大の分担金を拠出。

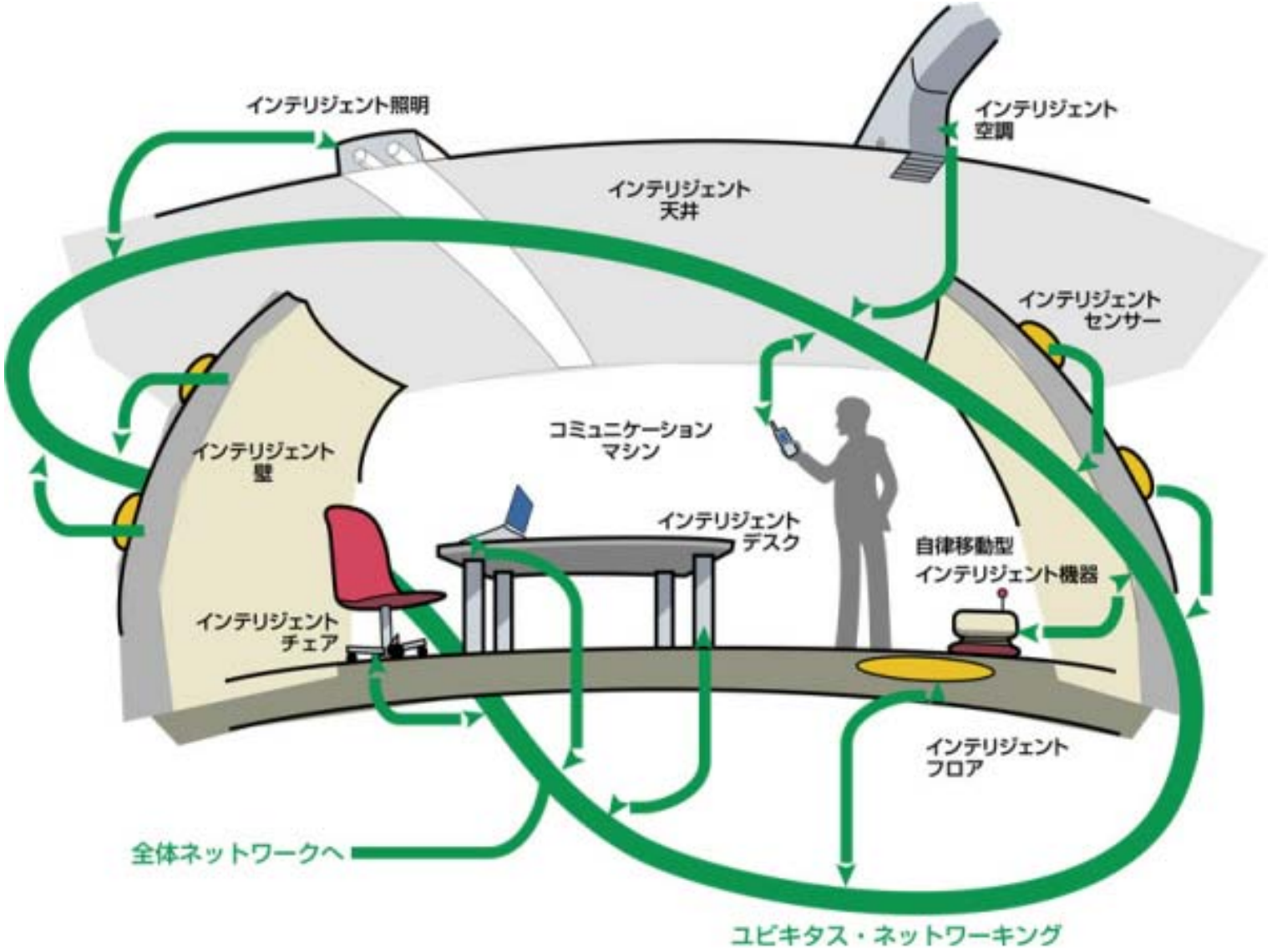
（参考2）ITU150周年賞

ITU創設150周年を記念して、過去から現在にわたりICTのイノベーション、促進、発展を通じて、世界中の人々の生活向上に多大な功績のあった個人を顕彰するために設けられた賞。

出展：総務省ホームページ

Copyright © 2016 IPA, All Rights Reserved

30年前から存在したIoTのコンセプト



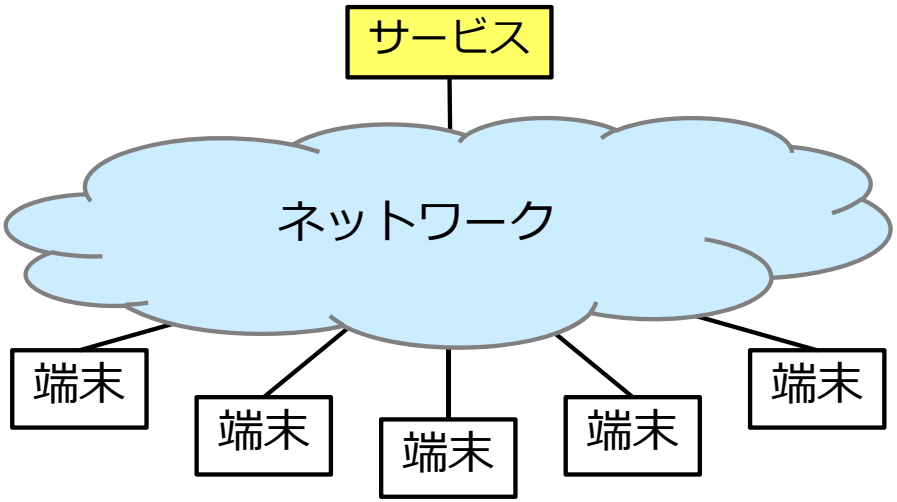
TRON Project1987 Open-Architecture Computer Systems 坂村健 編より

出展：T-Engine フォーラム

Copyright © 2016 IPA, All Rights Reserved

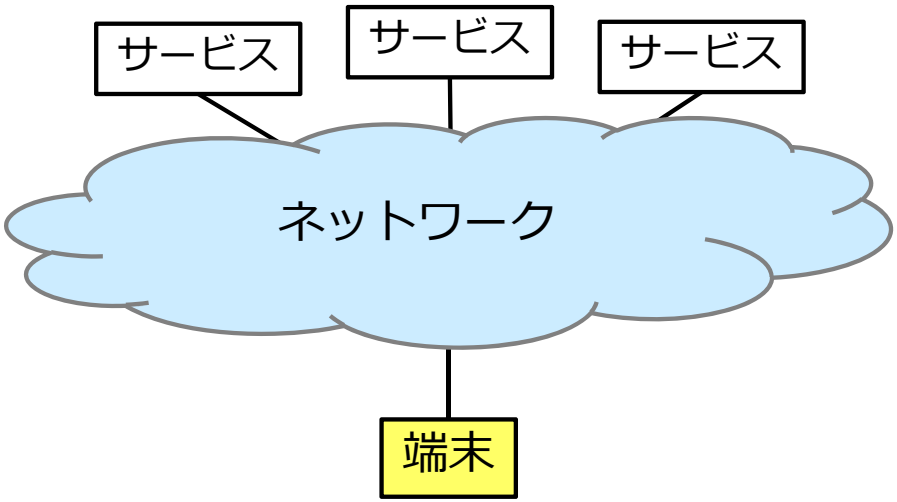
ステークホールダで見方が異なるIoT

サービスにとってのIoT



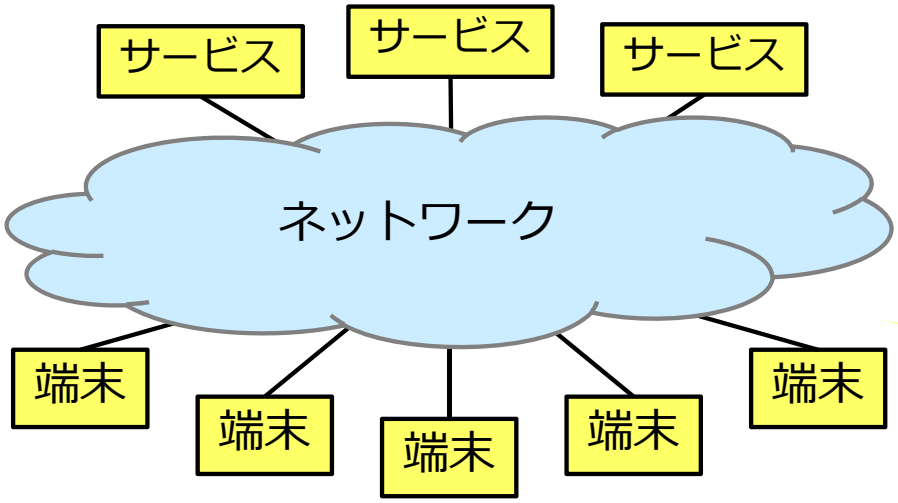
IoTで接続された数多くの端末から集めたビッグデータを活用して高度なサービスを提供します…

端末／ユーザにとってのIoT



IoTで接続された種々のサービスをワンストップで提供します…
必要なサービスを組合わせてお好みのスタイルで提供できます…

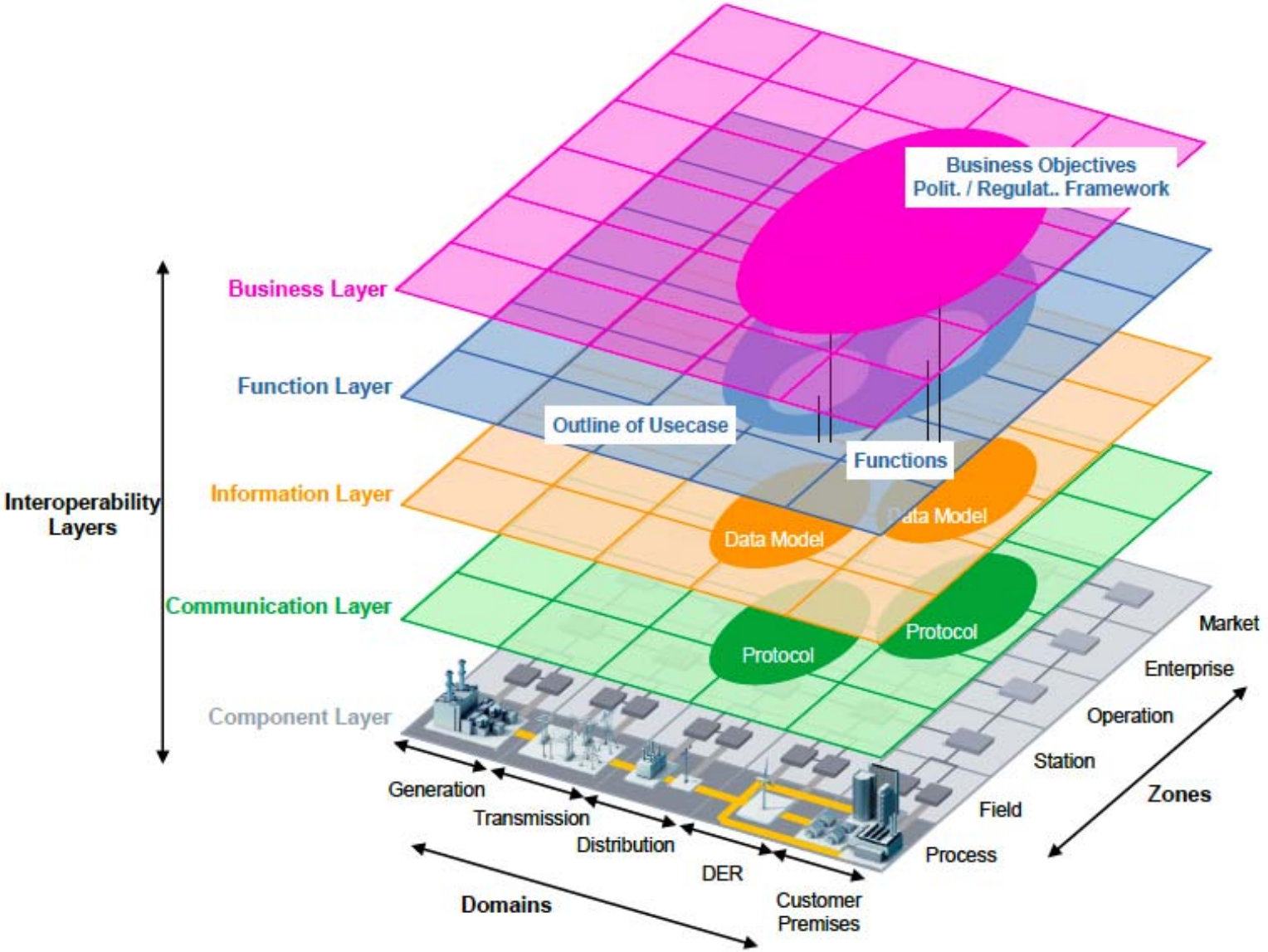
IoTの全体像



IoTでサービス同志も端末同志も繋がり…

Copyright © 2016 IPA, All Rights Reserved

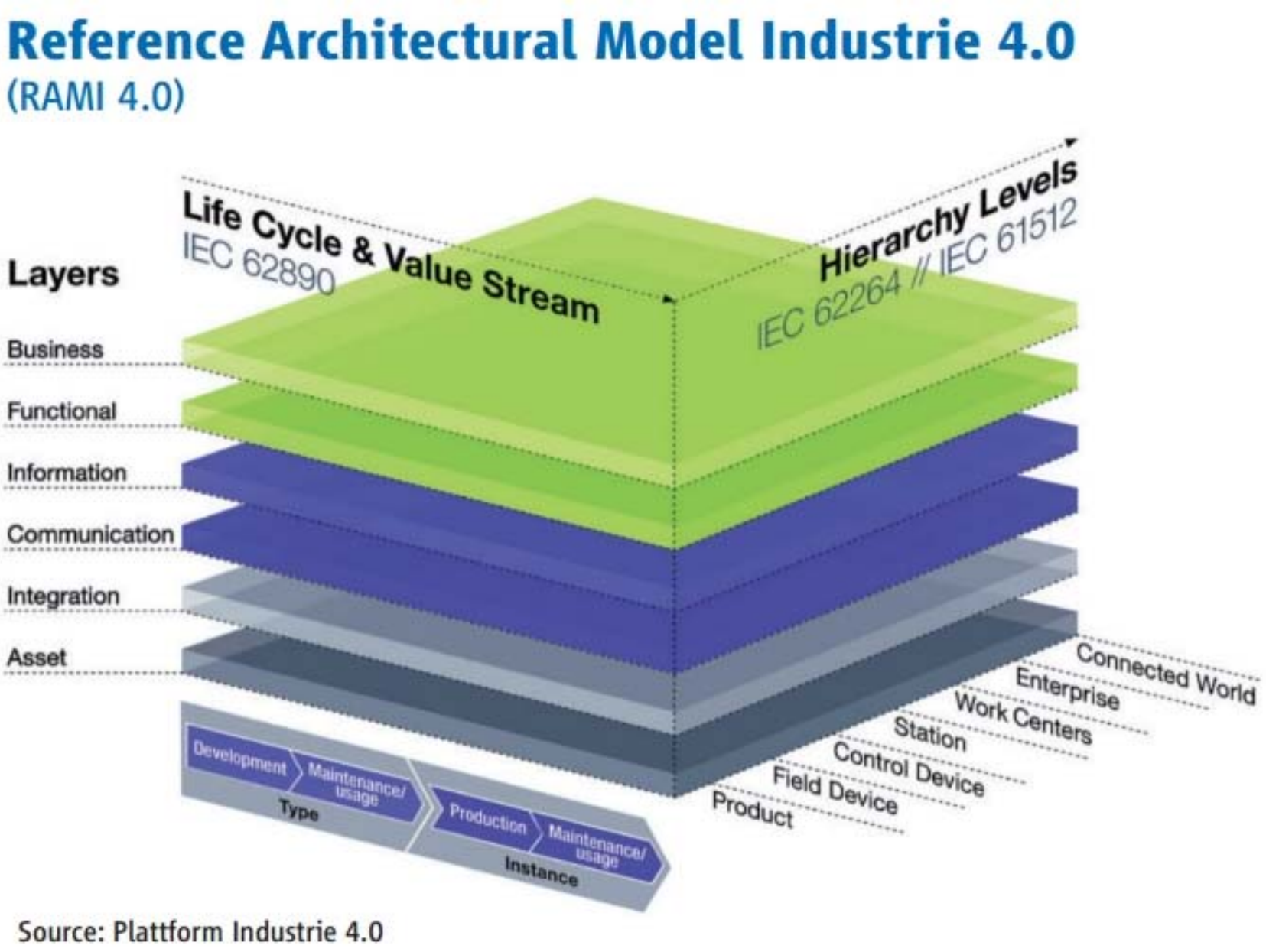
[ご参考] Smart Grid Reference Architecture



http://ec.europa.eu/energy/sites/ener/files/documents/xpert_group1_reference_architecture.pdf

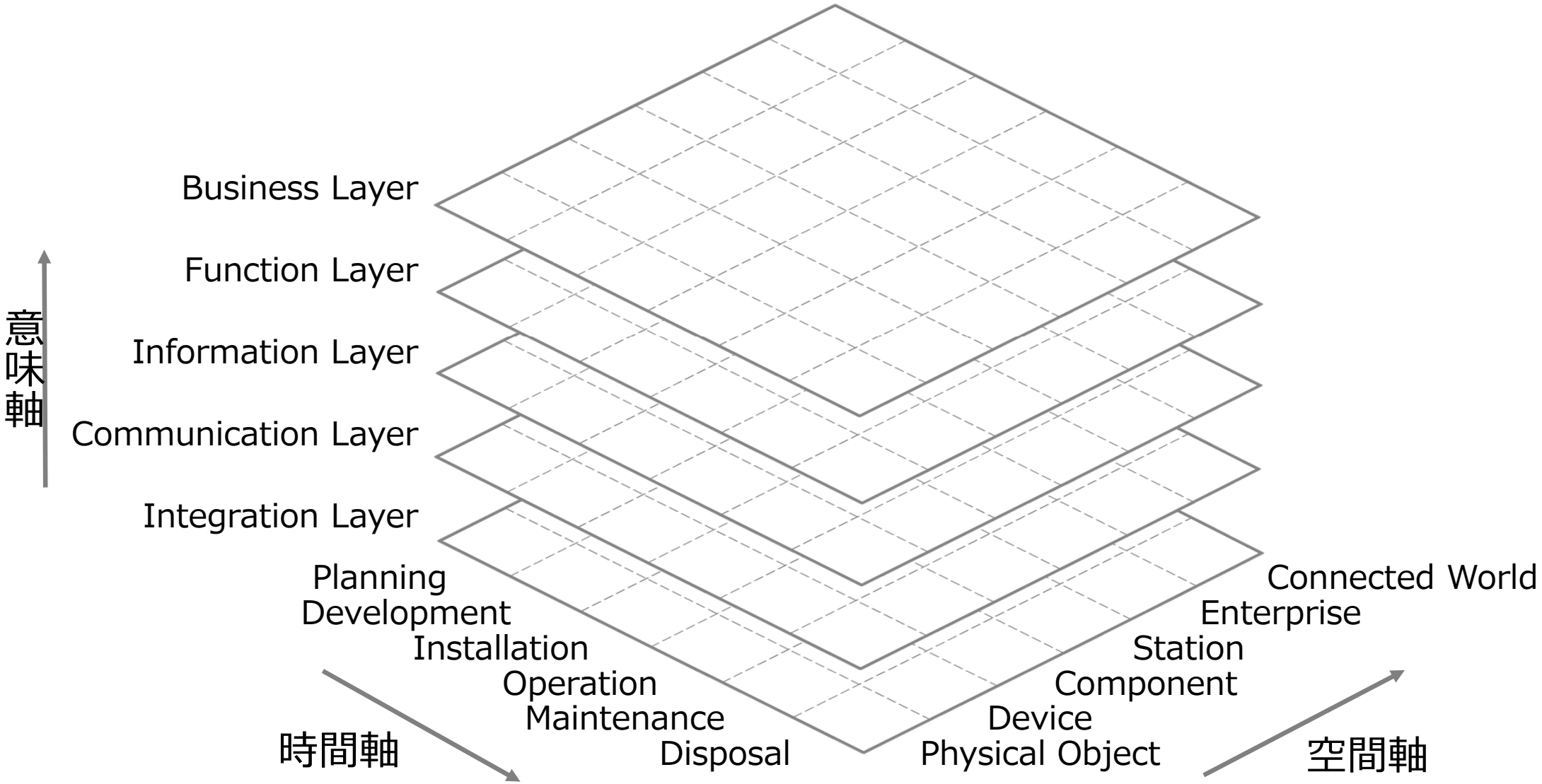
Copyright © 2016 IPA, All Rights Reserved

[ご参考] Industry 4.0 Reference Architecture



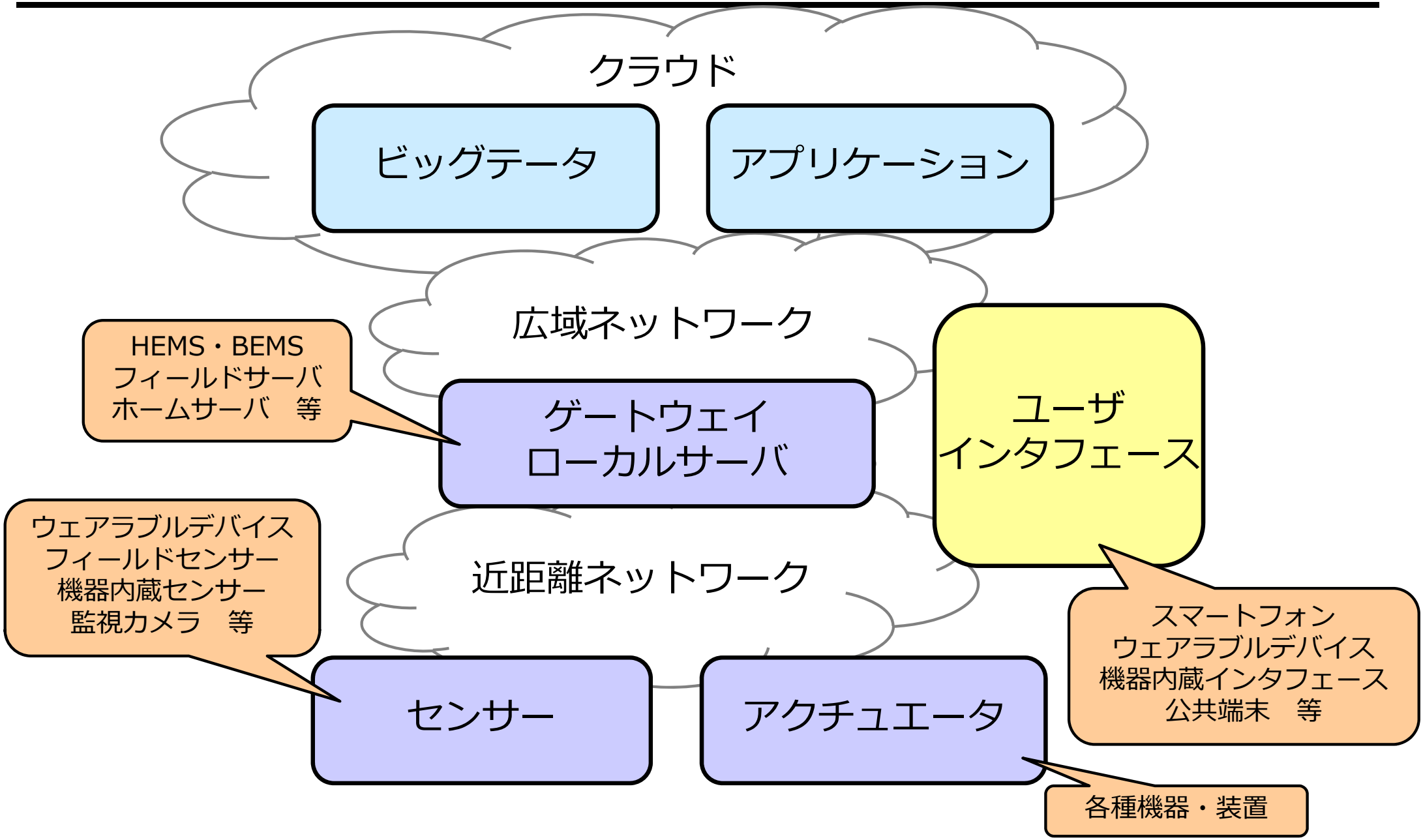
Copyright © 2016 IPA, All Rights Reserved

IoT の Reference Architecture



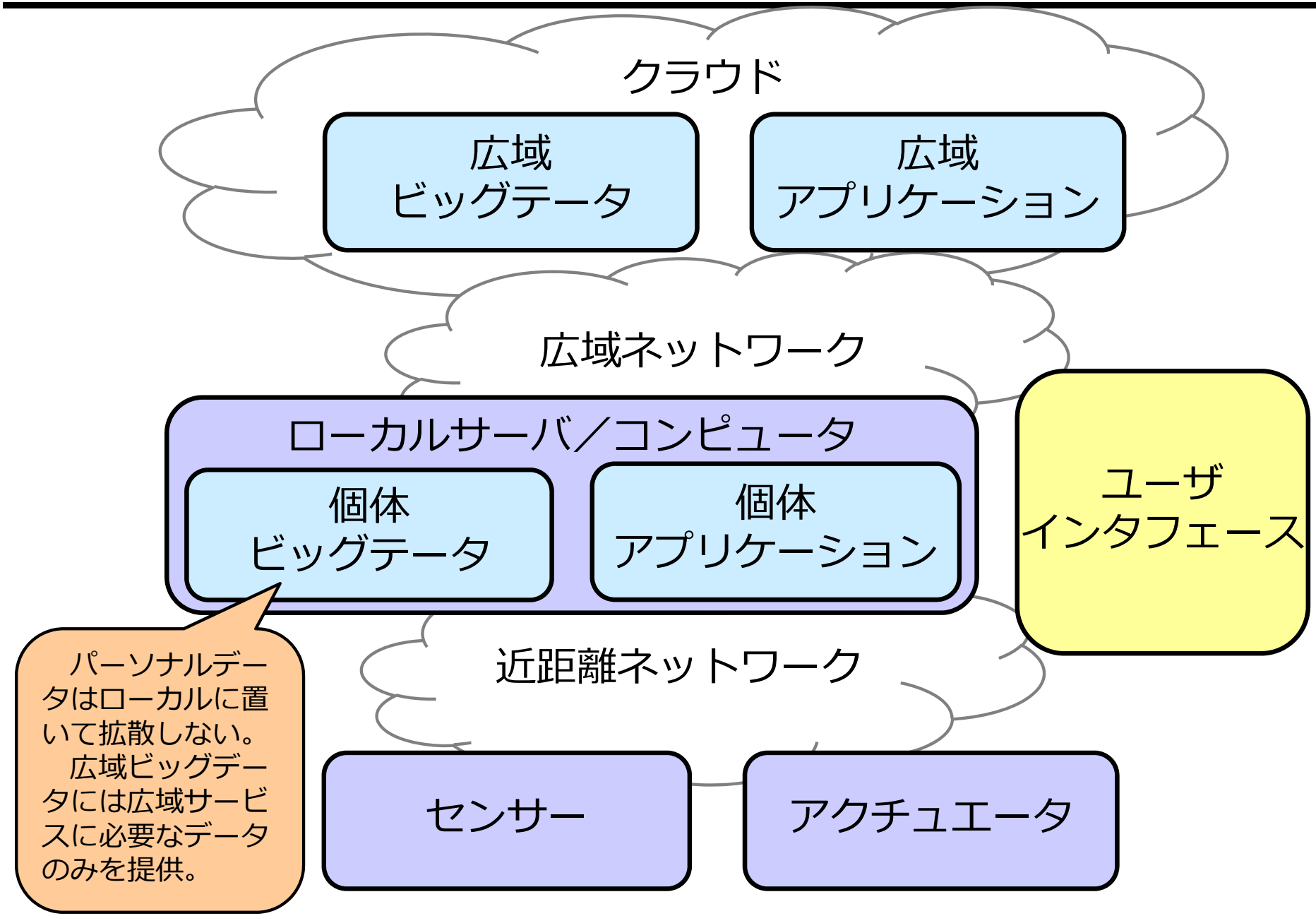
Copyright © 2016 IPA, All Rights Reserved

IoTシステムのシステム階層モデル



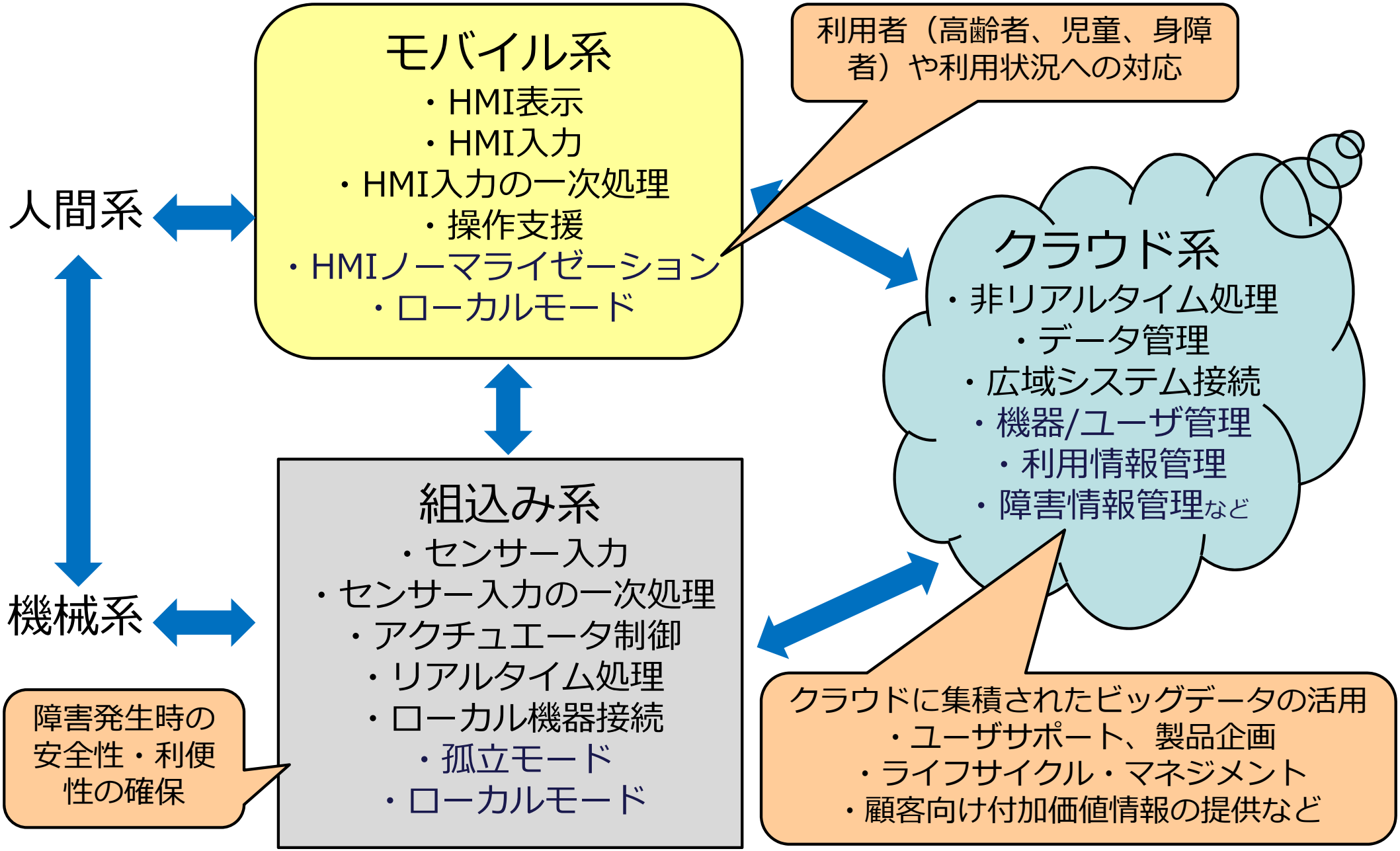
Copyright © 2016 IPA, All Rights Reserved

パーソナルデータを考慮したIoTシステム



Copyright © 2016 IPA, All Rights Reserved

IoTのシステム階層モデル要素の基本的な役割



Copyright © 2016 IPA, All Rights Reserved

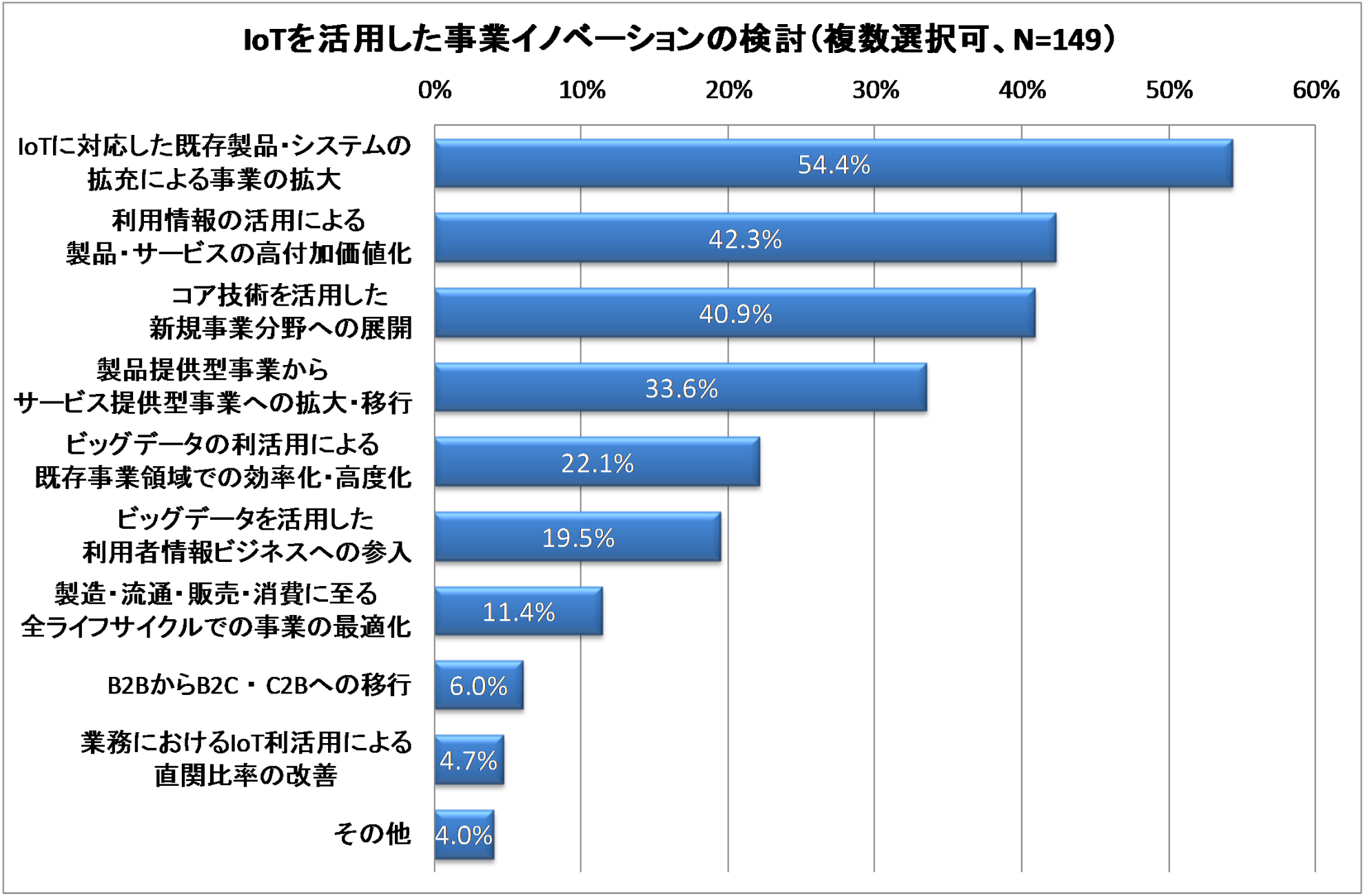
IoTの特徴とその課題に対応する技術キーワード

SEC
Software Reliability Enhancement Center

- 業界を跨ってシステムが連携してサービスを提供
  - システムエンジニアリング
    - ステークホールダ定義、要求獲得・要件定義
  - SQuaRE （ISO/IEC 25000 シリーズ）
    - システム品質、利用時品質、データ品質、運用品質
- 組込み、モバイル、クラウドがネットワークで接続
  - M2M
    - 無線技術（WiSUN、BLEなど）、センサー技術、フィールドネットワーク
  - ビッグデータ
    - 構築技術（データ品質確保、データ分類整理技術など）
    - 活用技術（ビッグデータ分析、データモデリング、個人情報保護など）
- 連携する個々のシステムが独立に新陳代謝しながら継続的に進化
  - モデルベース（SysML、MATLAB/Simulinkなど）
    - モデリング技術、モデルベース開発技術、モデルベース検証技術
  - 形式手法（形式的仕様記述とモデル検査）
  - IV&V（Independent Validation & Verification)と認証
- 一つの障害が広範囲に波及・影響するリスク
  - 機能安全とセキュリティ
    - リスク分析（FTA、FMEA、HAZOP、STAMP等）
  - アシュアランスケース（GSN、D-CASEなど）と障害対応（DEOSプロセスなど）

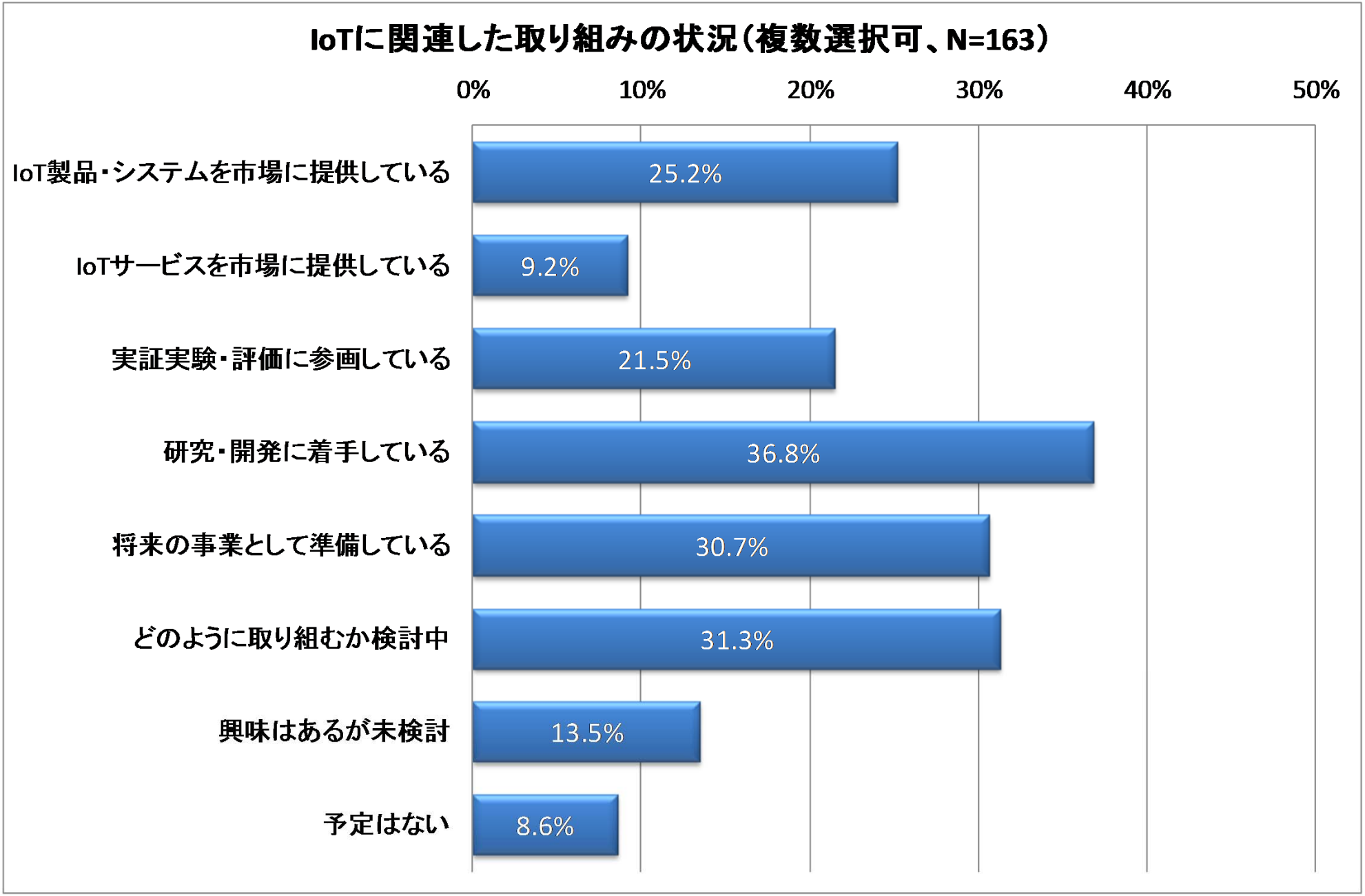
Copyright © 2016 IPA, All Rights Reserved

IoTを活用した事業イノベーション



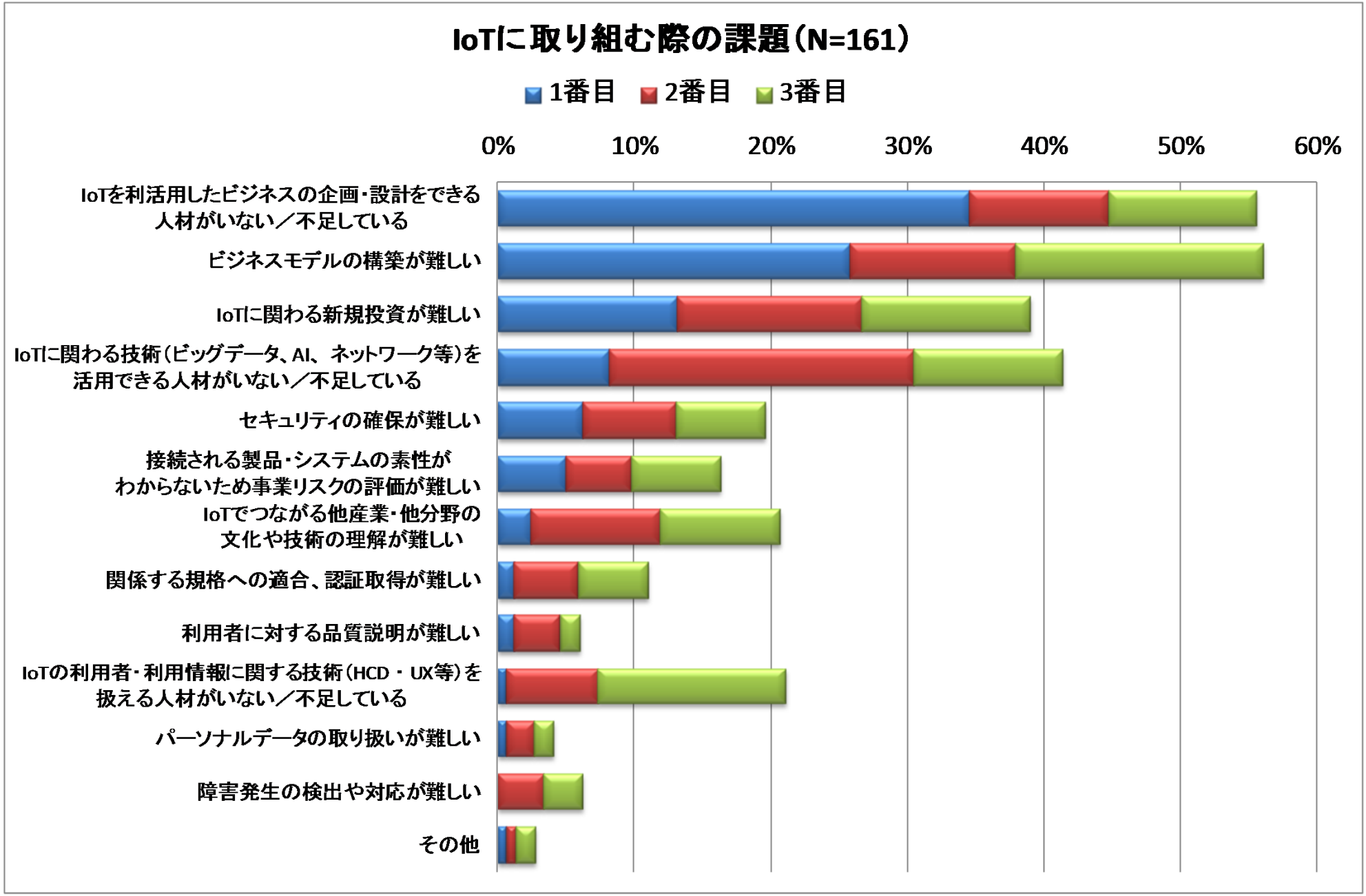
Copyright © 2016 IPA, All Rights Reserved

IoTに関連した取り組みの状況



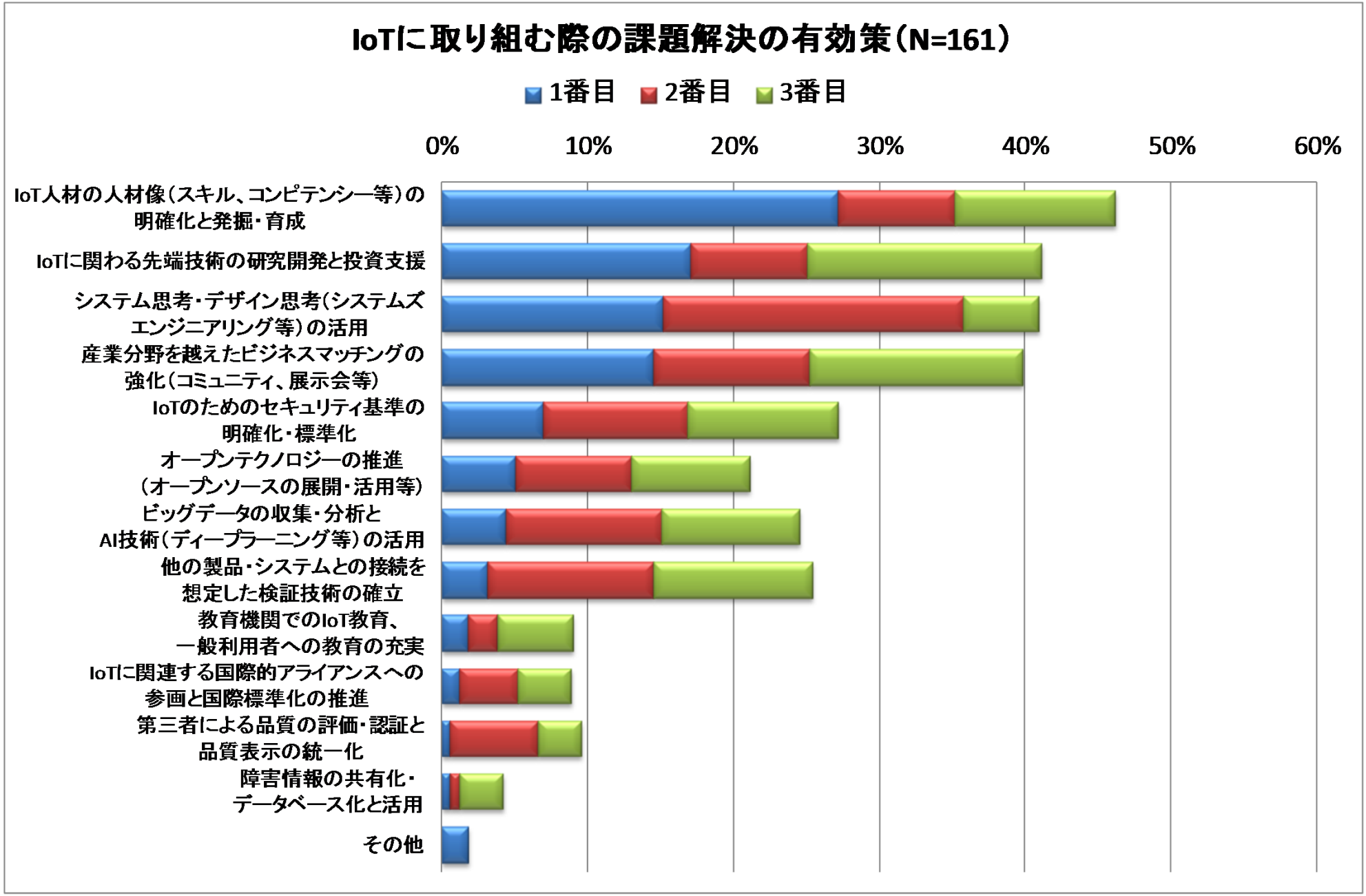
Copyright © 2016 IPA, All Rights Reserved

IoTに取り組む際の課題



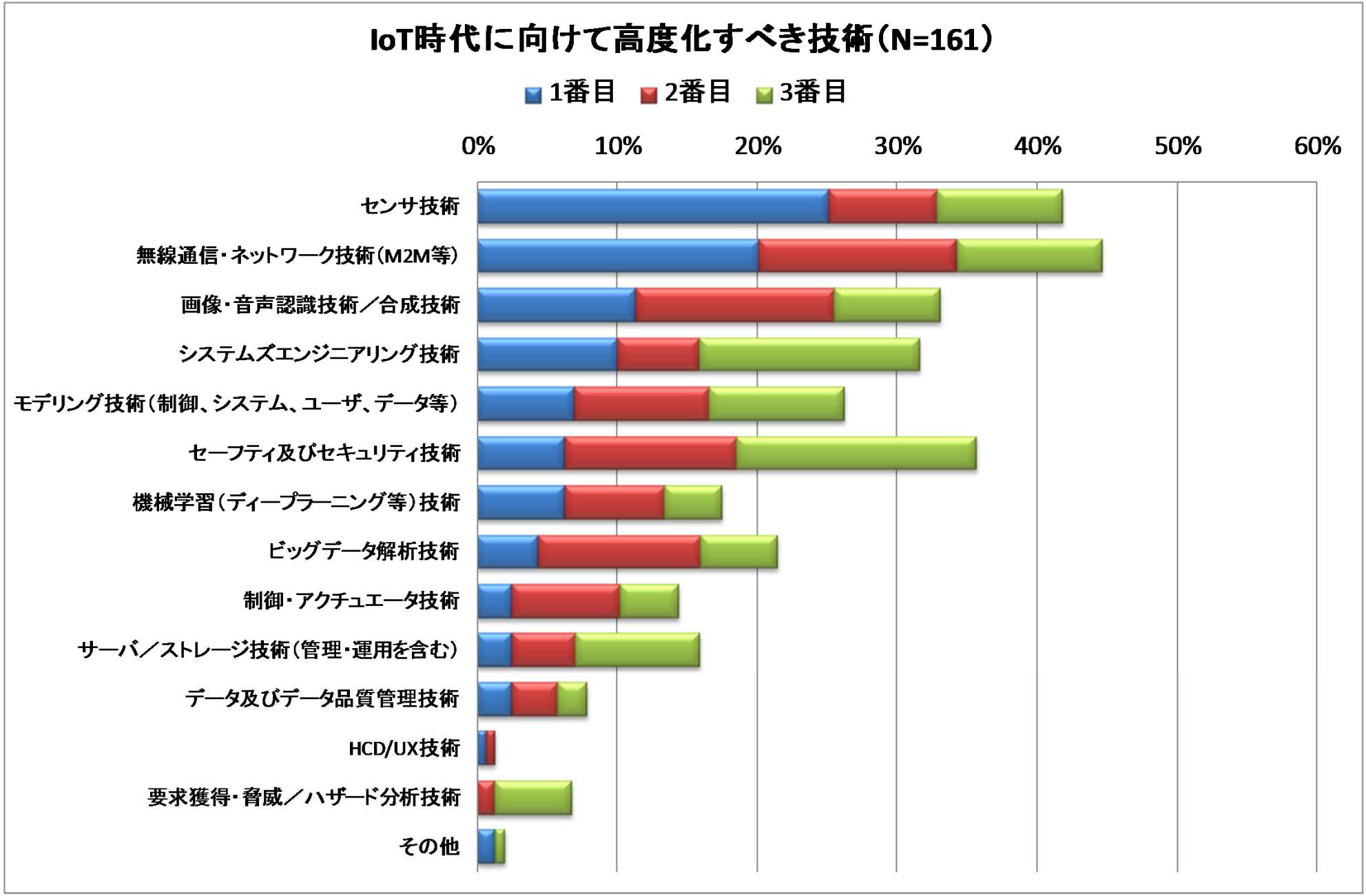
Copyright © 2016 IPA, All Rights Reserved

IoTに取り組む際の課題解決に有効な策



Copyright © 2016 IPA, All Rights Reserved

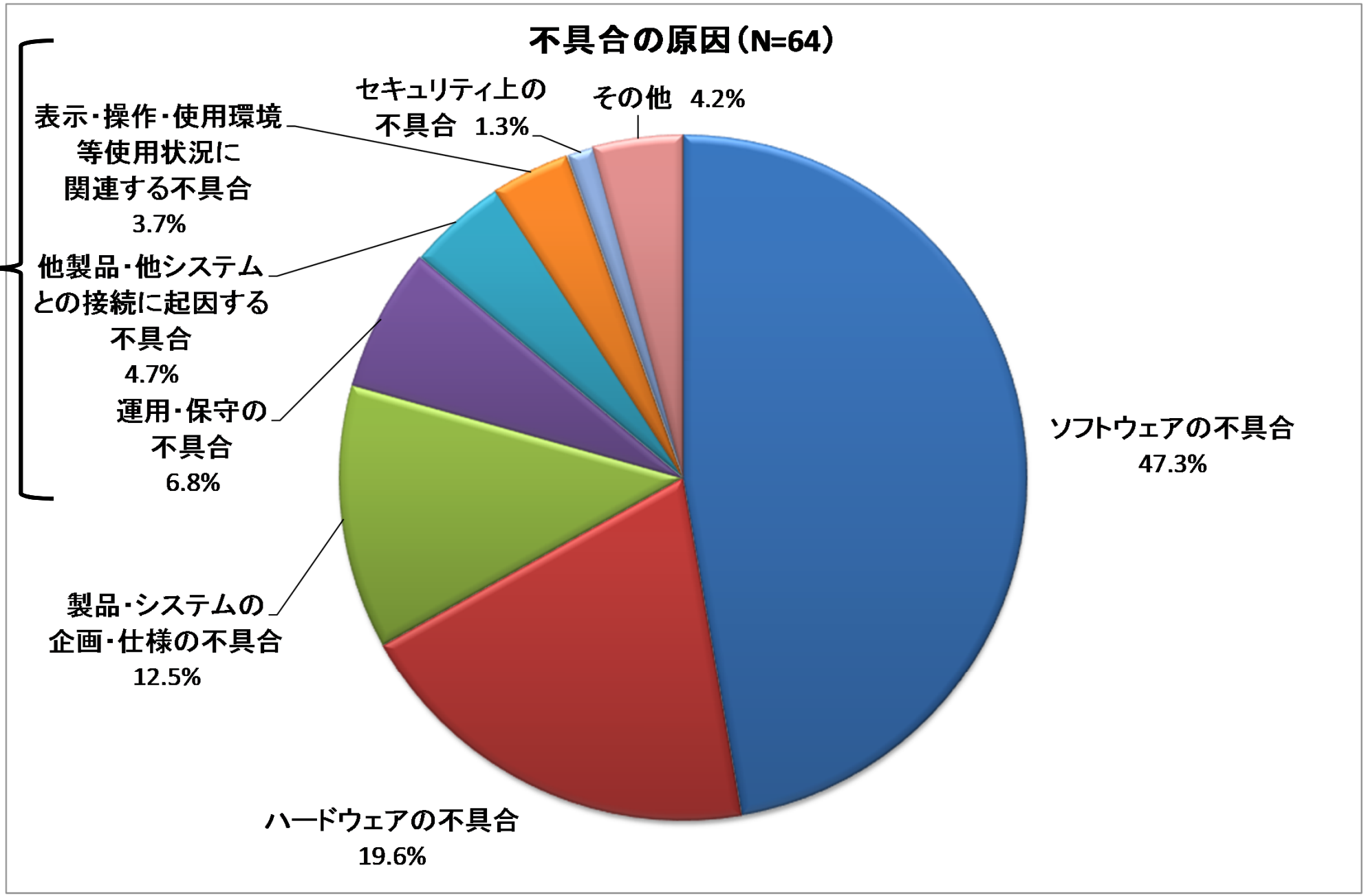
IoT時代に向けて高度化すべき技術



Copyright © 2016 IPA, All Rights Reserved

IoTの進展で更に増加が懸念される不具合

利用状況・利用環境に関連した不具合が増加傾向



Copyright © 2016 IPA, All Rights Reserved

機能しなかった多重安全システム
スリーマイル島原発事故（1978年3月）

SEC Software Reliability Enhancement Center

事故原因 ＝ 機器の故障 ＋ 運転員のヒューマン・エラー

The Reports of
The President's Commission On The Accident At Three Mile Island

The ***Report of the President's Commission on the Accident at Three Mile Island*** is just one of the documents produced by the commission and its staff. Over 30 other reports were published. Several are included here and others may be added in the future.

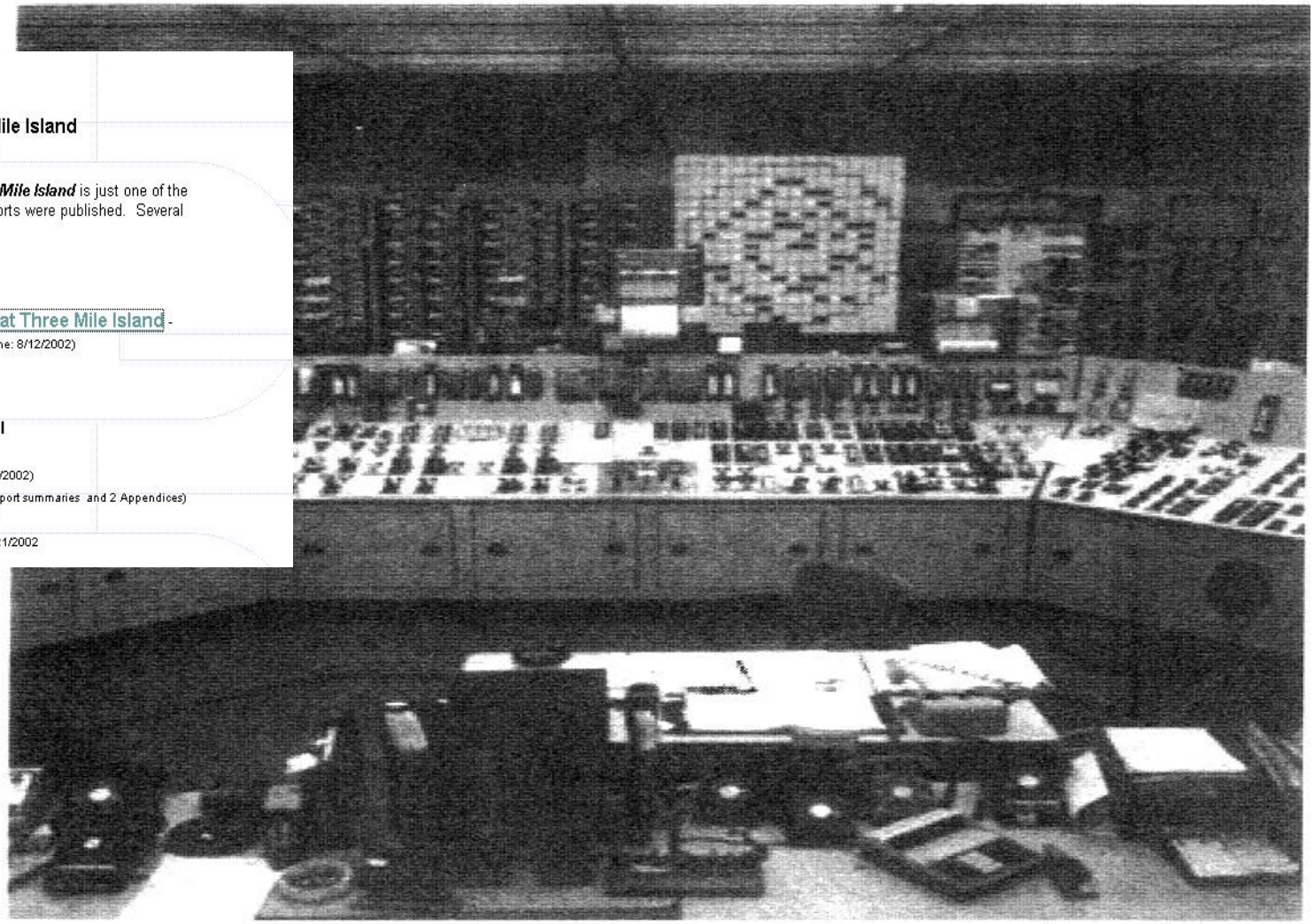
Reports:

Report of the President's Commission on the Accident at Three Mile Island - this is the report that was delivered to President Carter late in 1979. (online: 8/12/2002)

Staff Reports to the Commission

Reports of the Technical Assessment Task Force, Vol. I

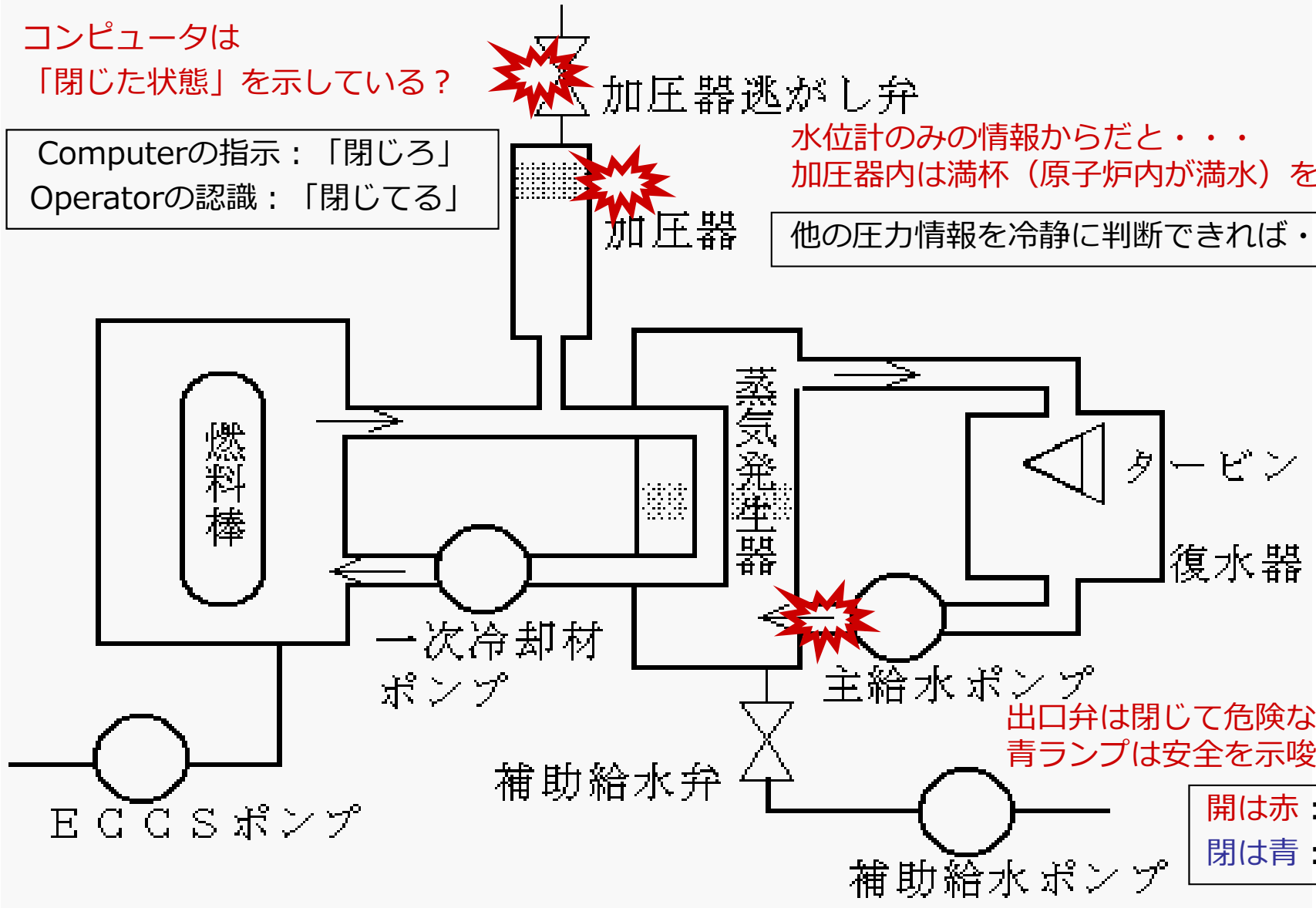
- Technical Assessment Task Force Staff (added 9/2/2002)
- Technical Staff Analysis Reports Summary 26 report summaries and 2 Appendices) (added 9/3/2002 to 9/8/2002)
- Summary Sequence of Events (added 9/9/2002 to 9/21/2002



The control room at the Three Mile Island nuclear power plant .[5]

Copyright © 2016 IPA, All Rights Reserved

表示系の問題点とヒューマンエラー箇所



TMI原発事故 吉田伸夫:http://www005.upp.so-net.ne.jp/yoshida_n/L5_02.htm

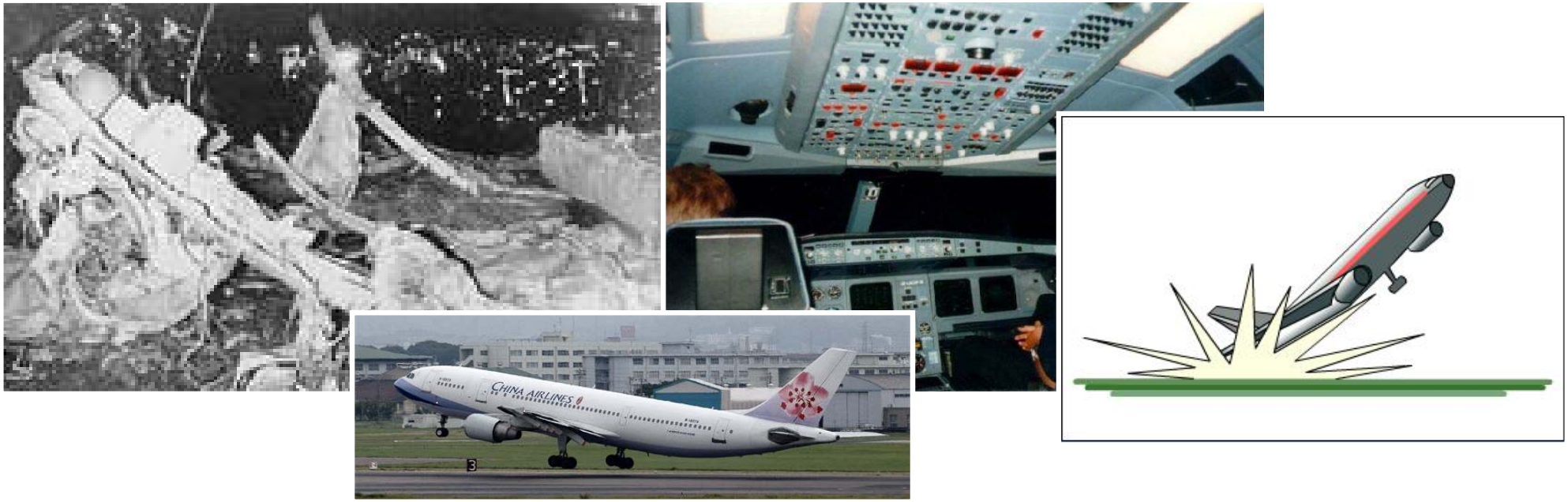
Copyright © 2016 IPA, All Rights Reserved

緊急時を想定しなかった自動化システム
エアバス事故A300型機事故（1994年4月）

SEC Software Reliability Enhancement Center

1994年4月26日、台北・中正国際空港発名古屋空港行きの中華航空機CI140便（エアバスA300-600R型機・登録番号B-1816）が、名古屋空港で着陸に失敗して墜落、乗客乗員271人のうち264人が死亡し7人が負傷。

着陸体制中に、副操縦士が誤ってゴー・アラウンド（着陸復行、着陸を一旦中止してやり直すこと）スイッチを作動させたことで機体が上昇、さらにゴー・アラウンドモードの解除に失敗したうえ自動操縦に逆らった操作をしてしまうなど、いくつもの人為的なミスが重なった結果、機体が急角度で上昇して失速、失速点からほぼ垂直に落下するような形で墜落に至った。



出典：ＥＵと企業関係～AIRBUS（エアバス）社にみる企業とEU（K.R.Rep.No.2）

Copyright © 2016 IPA, All Rights Reserved

緊急時を想定しなかった自動化システム
エアバス事故A300型機事故

SEC Software Reliability Enhancement Center

複雑な航空機のシステム
特に自動化したシステムとパイロットの意思疎通
緊急時には簡単なロジックでさえ思い出すことは極めて困難

1994年4月26日　名古屋空港

意図せずにセットされたゴーアラウンド・モード→ランディング・モードに変更

パネルの「LAND」スイッチを何度も押す→モードを変更できず。

●設計者たちの考え方

一度ゴーアラウンド・モードをランディング・モード変更することは、普通の運航としてあり得ない

あるとするとそれはパイロットエラ→スイッチを押下しても操作を受け付けないという設計思想

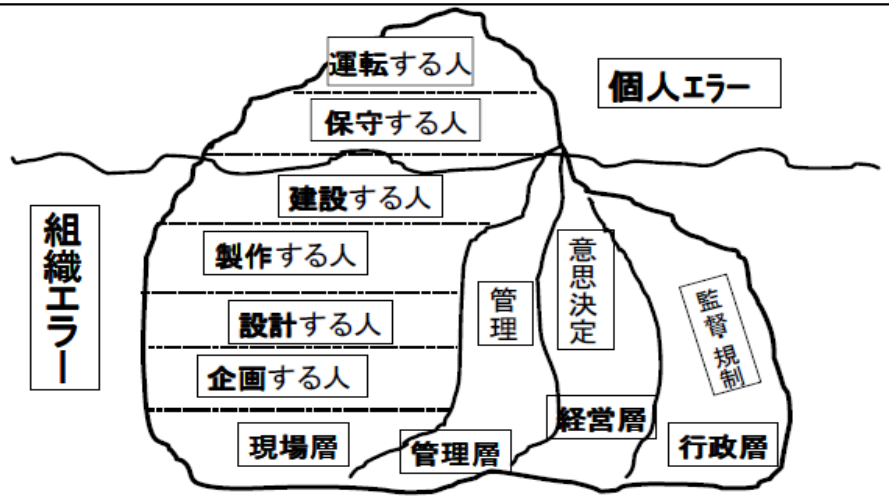


図 8　ヒューマンエラーの重層階層（Source 不明）

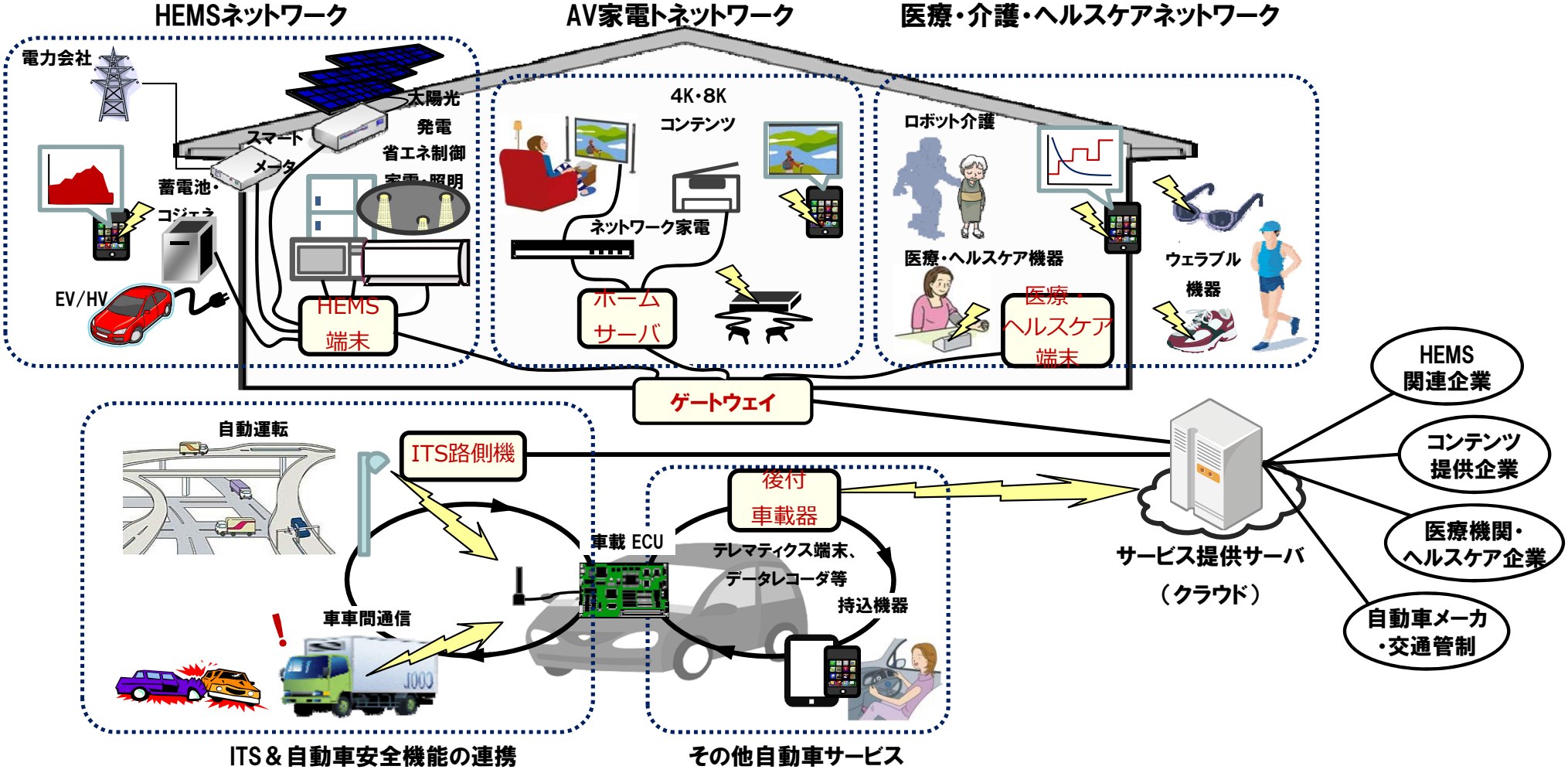
出典：社団法人日本流体力学会 ながれ21（2002）274 279.〔総合講座ながれより〕
飛行機はなぜ墜ちるか―航空安全のシステム
Why Airplanes Crash? – Human Factors Consideration in Airline Safety Management –
全日本空輸株式会社 総合安全推進部　十亀　洋

出典：国土交通省航空・鉄道事故調査委員会
中華航空A300-622R事故報告書1996

Copyright © 2016 IPA, All Rights Reserved

想定される2020年の社会

- 既に導入が始まっているHEMS、AV家電、医療・ヘルスケア、自動車などの製品・サービスの普及が東京オリンピックに向けて加速すると想定される。

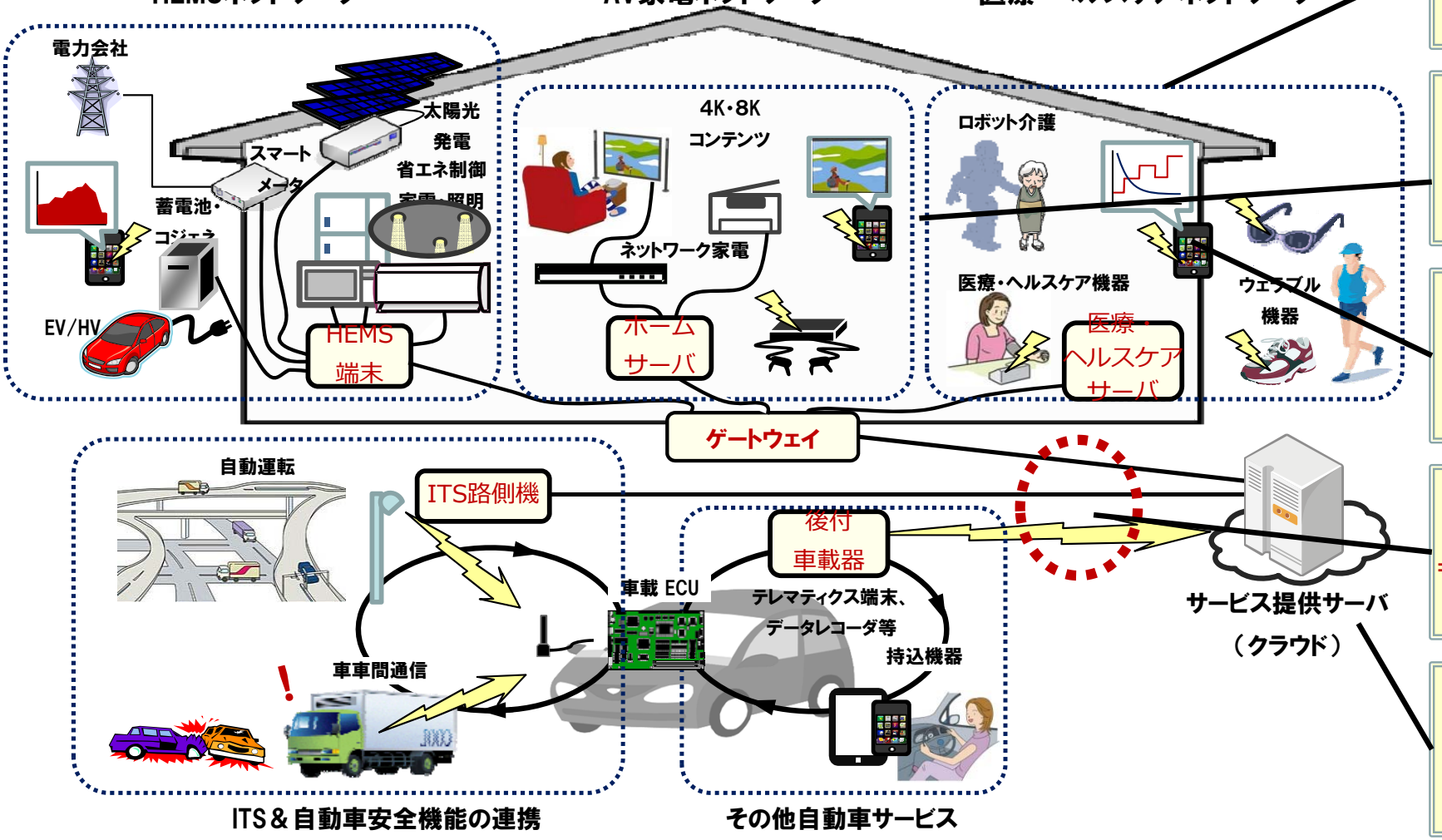


出典：一般社団法人重要生活機器連携セキュリティ協議会「セキュアライフ2020」より

Copyright © 2016 IPA, All Rights Reserved

2020年における脅威の想定

- 現状の脅威が「つながる」世界でさらに拡大、深刻化すると想定される。



何がつながっているか
分からない
＝脆弱性な生活機器が
攻撃の入口に

分野ネットワーク間の連携
ができていない
＝他分野の生活機器の
思わぬ動作が影響

いたる所で生活機器と
モバイルデバイスが接続
＝モバイルデバイスが
脅威の運び役に

多くの生活機器が
サーバと通信
＝プライベートに係る情報の
漏えい、改ざんの危険性

生活機器を遠隔から監視、
操作するサービスが増加
＝遠隔サーバの乗っ取りに
よる生活機器への攻撃も

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」より

Copyright © 2016 IPA, All Rights Reserved

信頼できるIoTの実現に向けて

SEC Software Reliability Enhancement Center

- 全体システムを意識したハザード・リスク分析　・・・　上流からの品質の確保
  - ハザード・リスク分析のスコープ
    - システム特性の利用者の期待との不整合
    - 機器の故障、設計の不良
    - 誤操作、錯誤等による人的ミス
    - 落雷、地震等の天災（大規模な機能喪失・不全）
    - セキュリティの脅威、意図的妨害、犯罪行為
  - ハザード・リスク分析の潜在リスク
    - ハザードの想定漏れ
    - ハザードとリスクとの対応付け漏れ
    - リスクの過小評価
- 品質の「見える化」「見せる化」　・・・　対他業界、対利用者、対社会
  - 「見える化」「見せる化」の対象
    - サブシステム（組込み、クラウド、モバイル）毎の品質
    - 全体システムの品質
    - 利用品質、利用者品質、データ品質　など
  - 「見える化」「見せる化」のための技術
    - 品質説明力の高い開発技術（形式手法、モデルベースなど）
    - エビデンス基づく管理技術（トレーサビリティー管理、アシュアランスケースなど）
    - 規格認証、第三者による検証・妥当性確認

Copyright © 2016 IPA, All Rights Reserved

信頼できるIoTの運用に向けて

SEC Software Reliability Enhancement Center

- 繋がるシステムの運用時に高まり続けるリスク
  - 市場で自由奔放に繋がり続けるシステムの繋がってしまったシステム間の相互作用による予期・予測できない障害等のリスクは増加し続ける
  - セキュリティリスクは市場投入から次第に増加
    - 攻撃手口・攻撃ツールの拡散、模倣犯の増加
  - サービス提供者はＩＴインフラの都合とは独立に事業を展開・発展
    - サービス提供者はＩＴインフラを構成するシステムの制約は意識しないのが一般的
- リスクモデルに対応した取組み
  - 従来の組込みシステムは、初期リスク（故障）と老朽化リスク（故障）の鍋底モデル
    ⇒　開発段階での取組みが重要
  - 繋がるシステムでは、出荷時から次第に増加し続けるリスクモデル
    ⇒　運用段階での取組みが重要
- 運用段階での取組みの課題
  - 開発期間より遙かに長い運用期間（例えば、期間開発は1-2年、運用は10年-20年）
    - 頼れない開発者の知見　⇒　属人性のない開発エビデンス、エビデンス間の関係
  - 業界を跨って繋がるシステム
    - 業界を超えた整合性の確保　⇒　運用プロセス、運用エビデンスの標準化（互換運用性確保）
  - リスクの拡大防止
    - 迅速な対応　⇒　対応の自動化、対応連鎖の形成

Copyright © 2016 IPA, All Rights Reserved

「つながる世界の開発指針」
安全安心なIoTの実現に向けて開発者に認識してほしい重要ポイント

SEC Software Reliability Enhancement Center

IoT機器/システムの開発者が安全/安心の確保のために最低限検討して欲しい事項を17の指針として整理。

「つながる世界の開発指針」の内容

目次：
- 第一章 つながる世界と開発指針の目的
- 第二章 開発指針の対象
- 第三章 つながる世界のリスク想定
- 第四章 つながる世界の開発指針（17指針）
- 第五章 今後必要となる対策技術例

※各指針毎にポイント・解説・対策例を記載

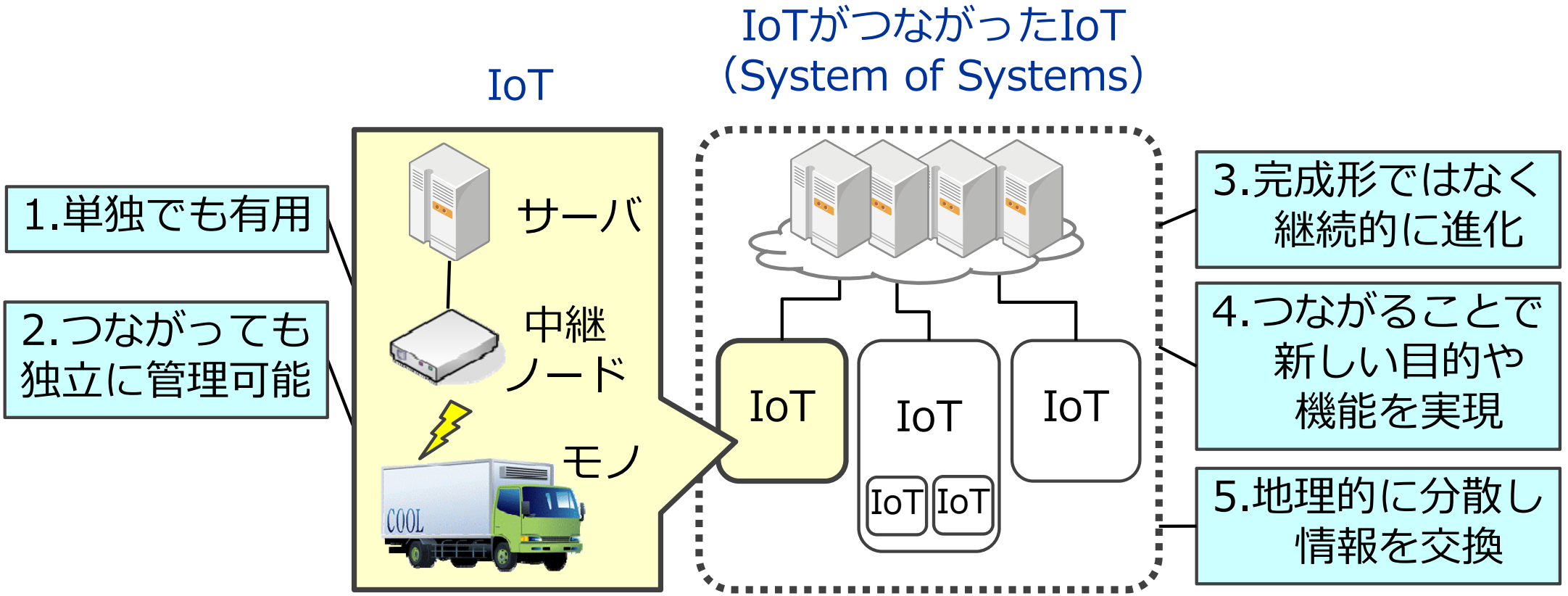
http://www.ipa.go.jp/files/000051411.pdf

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

Copyright © 2016 IPA, All Rights Reserved

開発指針でのIoTの捉え方

◆あらゆる「モノ」がネットワークにつながり、新しい価値を創生
◆さらに 、IoT同士がつながることで、新しい価値を創生



つながりにより拡大するリスクも発生

Copyright © 2016 IPA, All Rights Reserved

つながる世界の開発指針の狙い

SEC Software Reliability Enhancement Center

IoTの例：

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

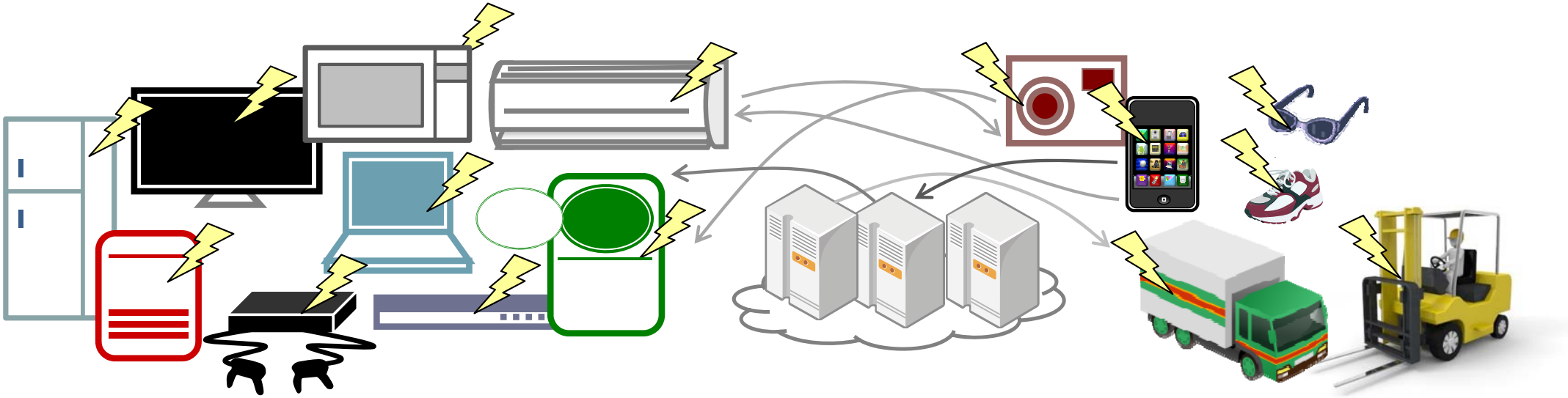
→ **IoT時代の安全と安心への危惧**

つながる事を想定して安全・安心を確保する設計が重要

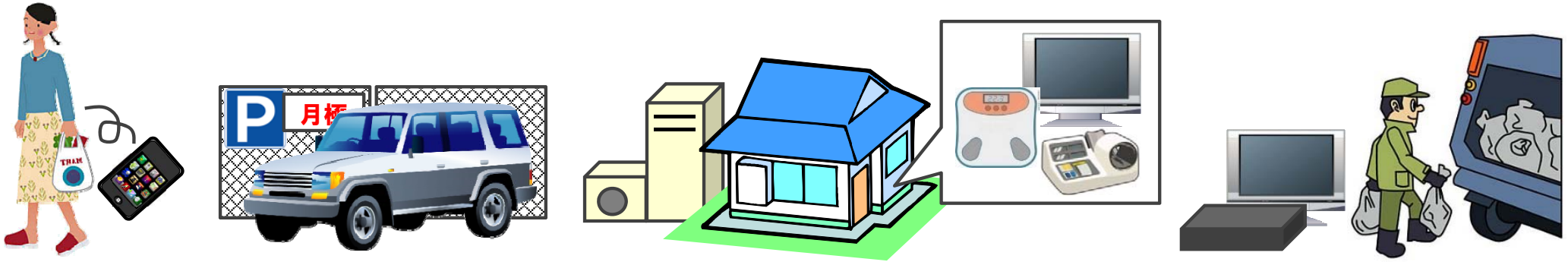
Copyright © 2016 IPA, All Rights Reserved

つながる世界の潜在リスク（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

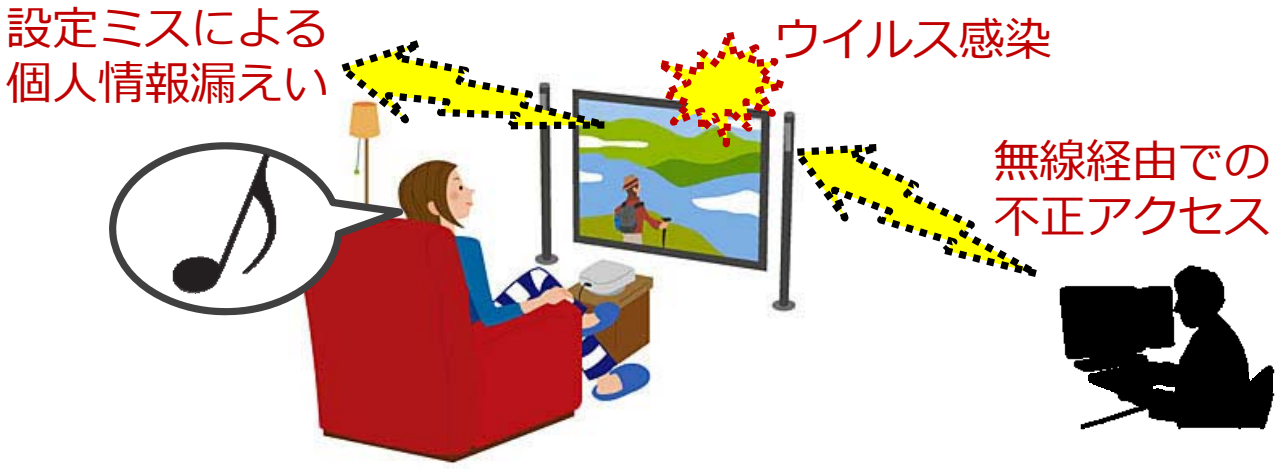


Copyright © 2016 IPA, All Rights Reserved

つながる世界の潜在リスク（２／２）

危害がつながりにより、身体や財産の危害にも波及する

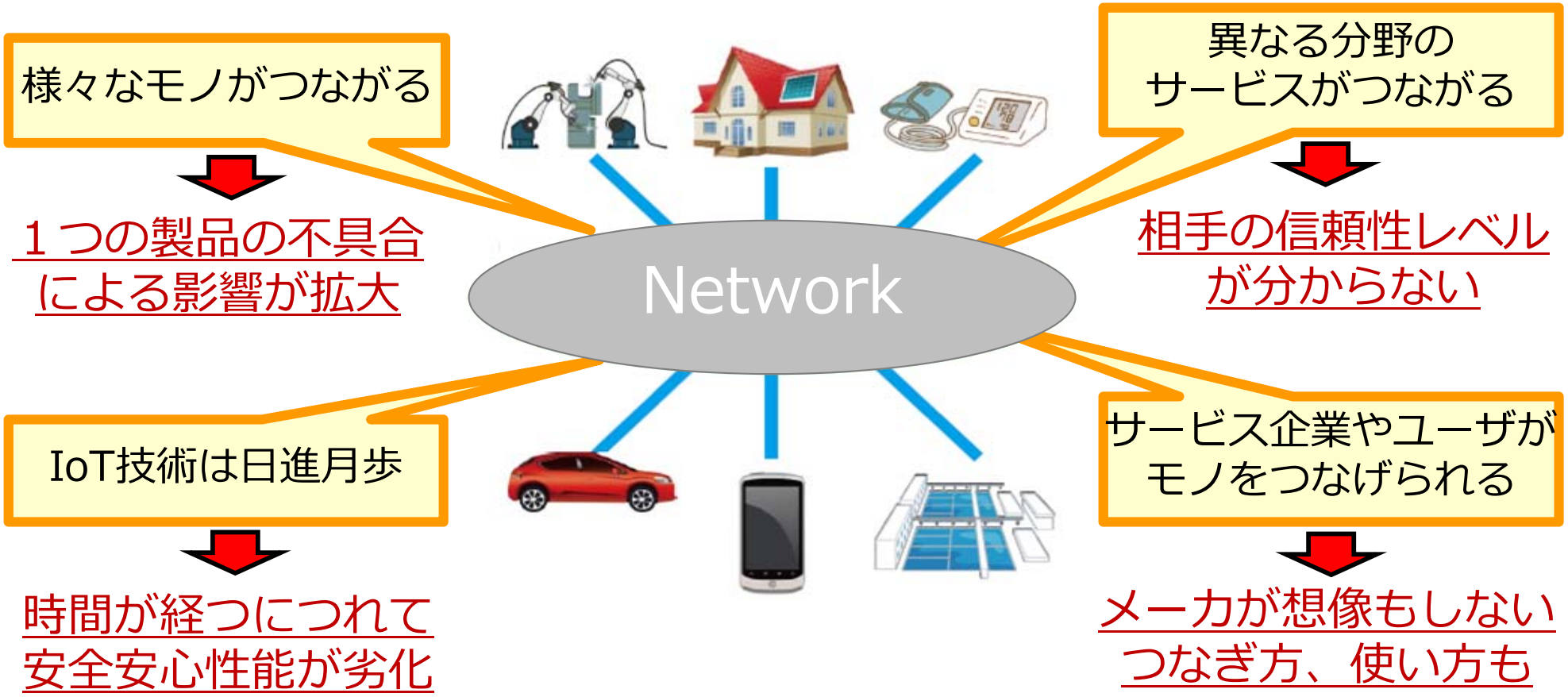
問題が発生してもユーザにはわかりにくい



Copyright © 2016 IPA, All Rights Reserved

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存在



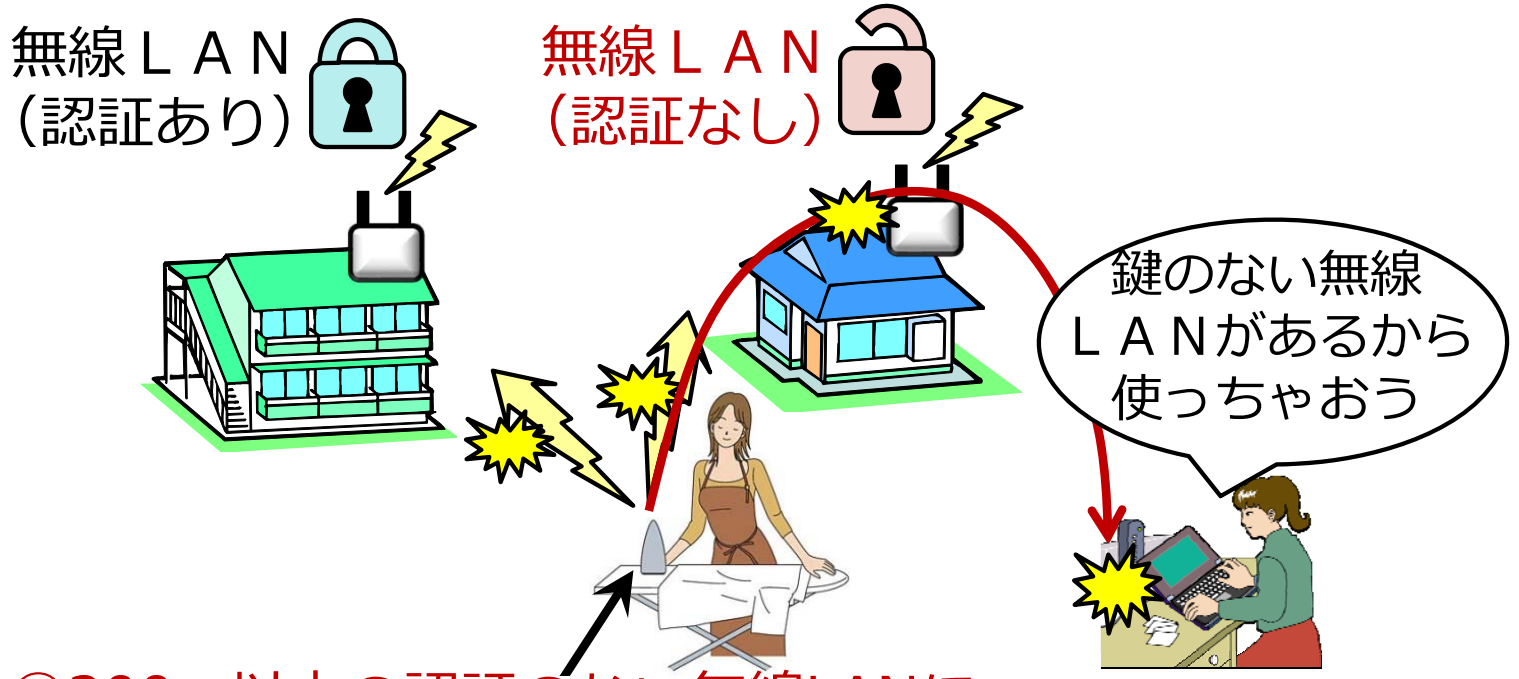
つながる世界のリスクを認識し、安全・安心への対策が必要

Copyright © 2016 IPA, All Rights Reserved

つながる世界のリスク（事例１）

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。

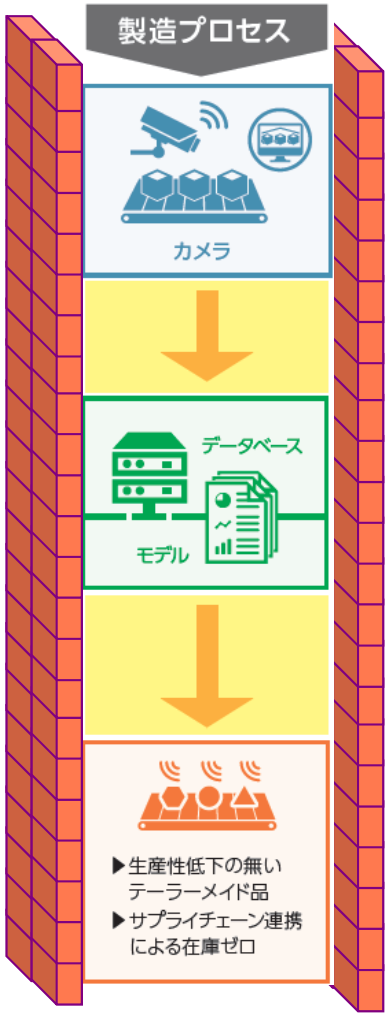


出典：一般社団法人 重要生活機器連携セキュリティ協議会「生活機器の脅威事例集」

Copyright © 2016 IPA, All Rights Reserved

つながる世界のリスク（事例２）

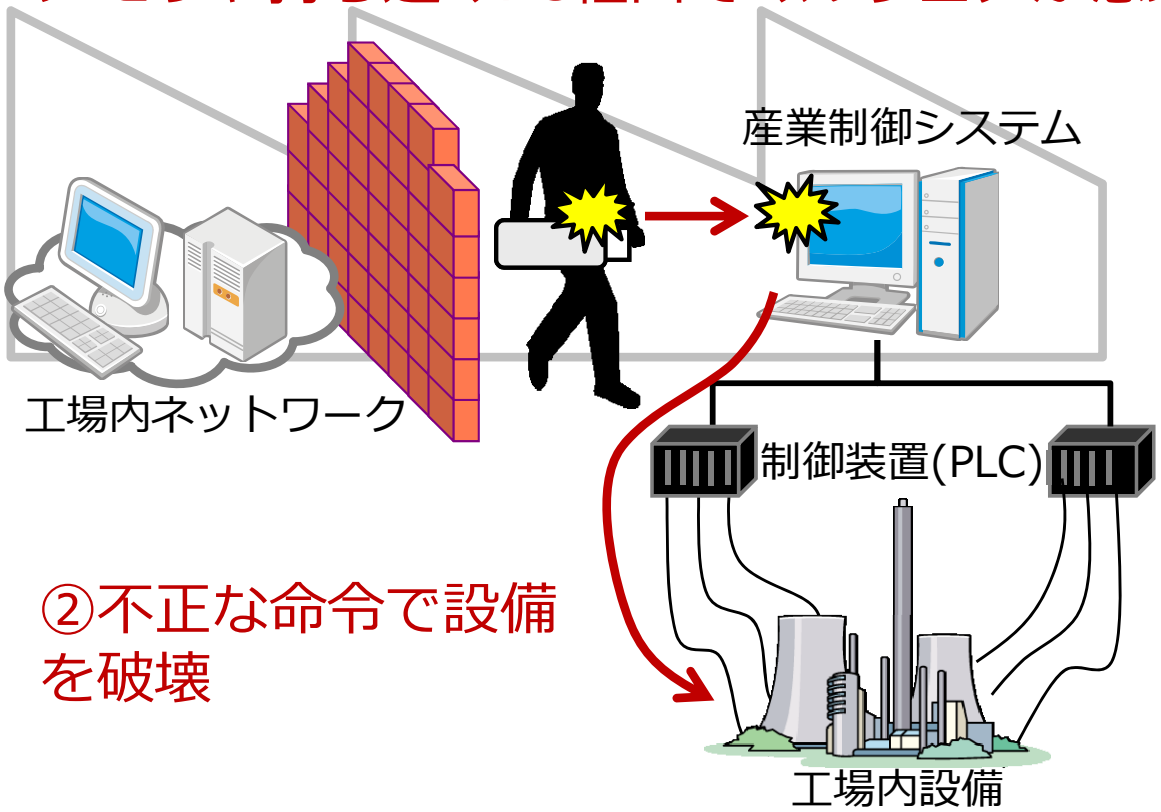
「つながらない」つもりなのに「つながってしまう」



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



②不正な命令で設備を破壊

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」

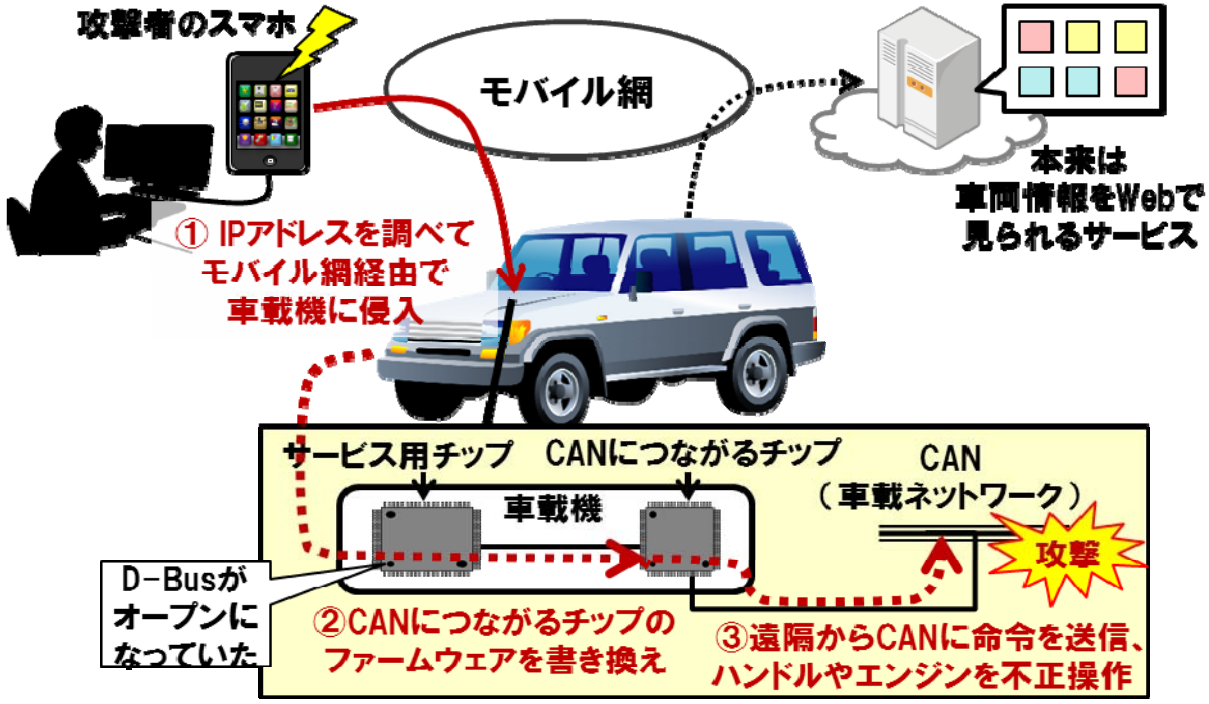
Copyright © 2016 IPA, All Rights Reserved

つながる世界のリスク（事例３）

出典：https://blog.kaspersky.co.jp

米国blackhat2015で発表があった自動車の攻撃研究の事例

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)

Copyright © 2016 IPA, All Rights Reserved

開発指針の概要

SEC
Software Reliability Enhancement Center

大項目		指針
方針	4.1 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　（方針策定）
		指針2　安全安心のための体制・人材を見直す　（体制構築）
		指針3　内部不正やミスに備える　（企業文化の醸成）
分析	4.2 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　（対象の特定）
		指針5　つながることによるリスクを想定する　（つなぐリスクの想定）
		指針6　つながりで波及するリスクを想定する　（波及リスクの想定）
		指針7　物理的なリスクを認識する　（物理的リスクの認識）
設計	4.3 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　（多重防御）
		指針9　つながる相手に迷惑をかけない設計をする　（波及防止）
		指針10 安全安心を実現する設計の整合性をとる　（設計の整合）
		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　（未知対応）
		指針12 安全安心を実現する設計の検証・評価を行う　（検証・評価）
保守	4.4 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　（状態把握）
		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　（経年維持）
運用	4.5 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　（情報収集・発信）
		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　（関係者への伝達）
		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　（利用者の啓発）

Copyright © 2016 IPA, All Rights Reserved

開発企業における開発指針の使い方

SEC Software Reliability Enhancement Center

開発指針の構成

開発指針

ポイントは必ず検討すべき項目

参考となる対策例
対策の実施は当事者の判断

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。
- チェック結果を取り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

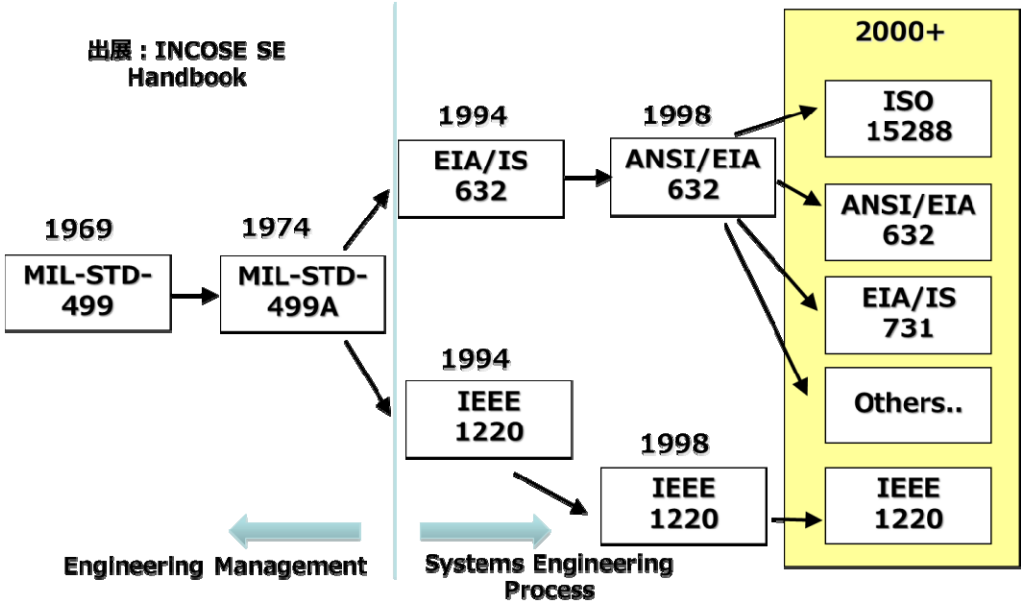
①外部インタフェース経由／内包／物理的接触によるリスクへの対策

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

Copyright © 2016 IPA, All Rights Reserved

システムエンジニアリングとは？

- 大規模・複雑なシステムを系統的に開発する体系。
- アポロ計画を着実に遂行するために体系化されたものが発展。当初、マネジメント主体であったが、1990年以降はプロセス主体に移行、2000年後半以降は、プロジェクト企画・計画など上流に範囲を広げるなど、大規模化・複雑化するシステムに対応して発展している。
- 物事をシステムとして捉えることで、ソフトウェアシステムやハードウェアシステムだけでなく、新規事業の開発、社会システムの設計など、様々な領域に適用可能。
- 業界を跨り構築される大規模・複雑なIoTシステムの開発やCPS社会のデザイン等では、有効で必須の体系として着目されている。

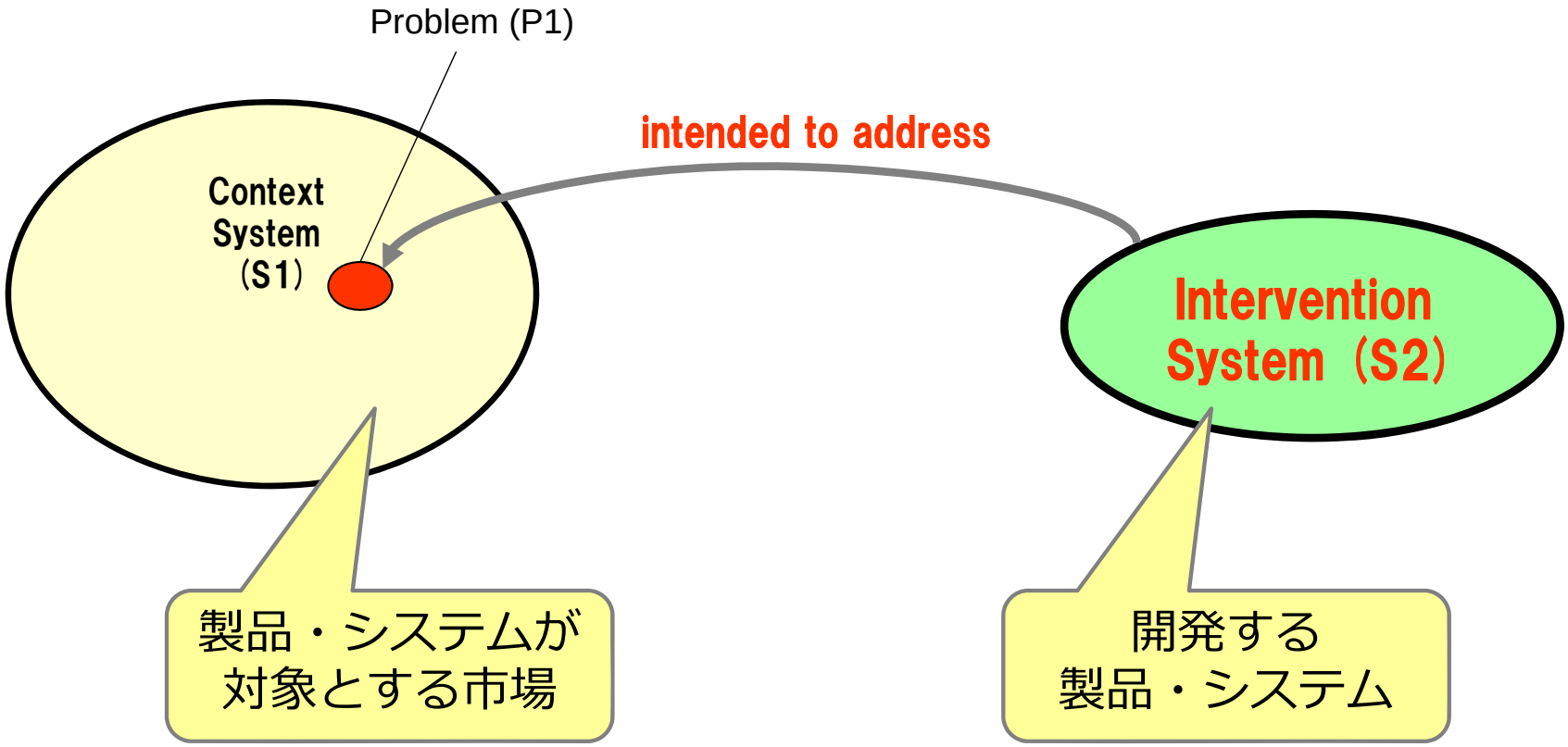


システムエンジニアリングの歴史

最新のシステムエンジニアリングの御三家

Copyright © 2016 IPA, All Rights Reserved

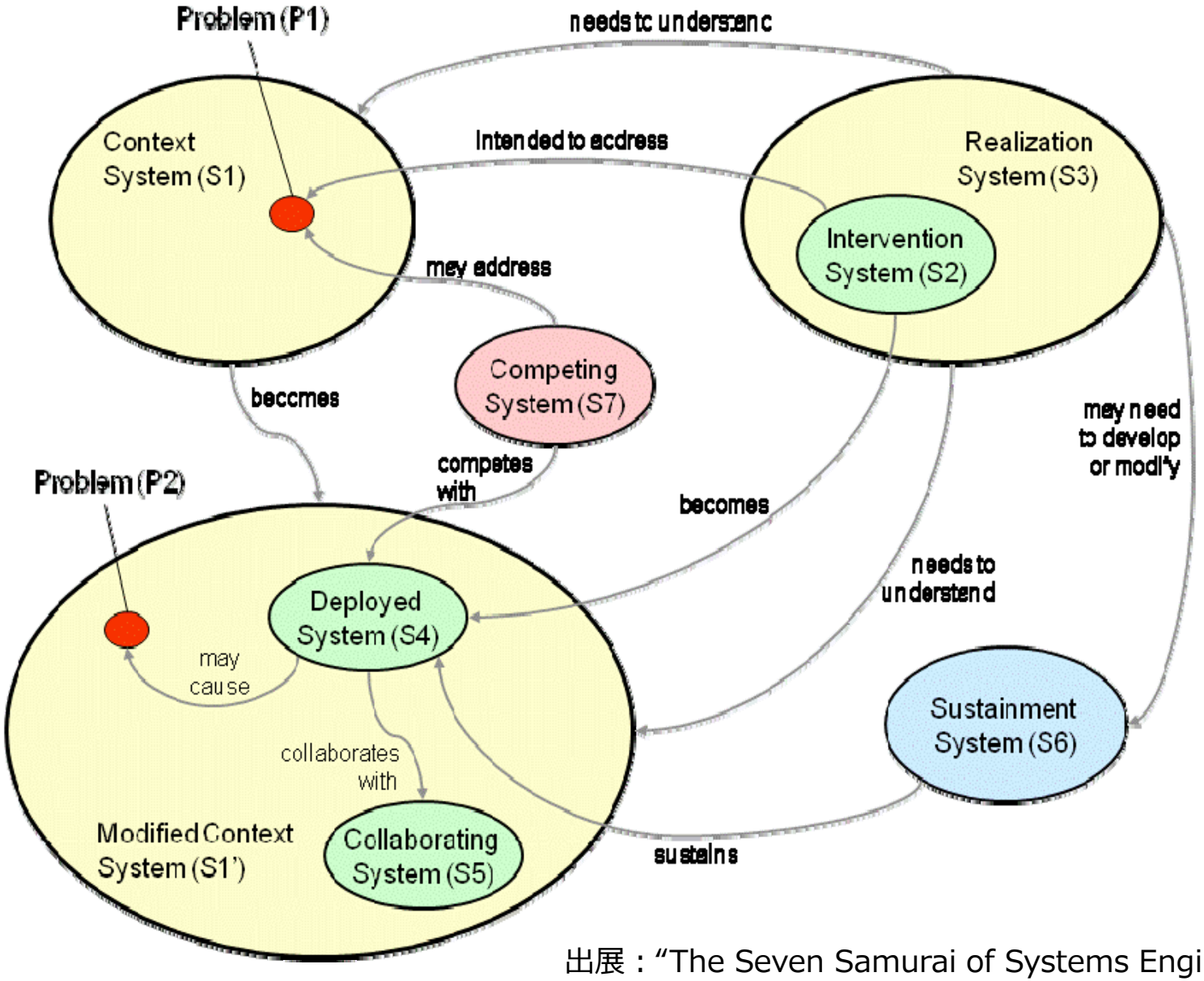
従来の組込みシステムのスコープ
Enterprise Systems Engineering: Seven Samurai



出展：“The Seven Samurai of Systems Engineering Dealing with the Complexity of 7 Interrelated Systems” By James Martin に加筆

Copyright © 2016 IPA, All Rights Reserved

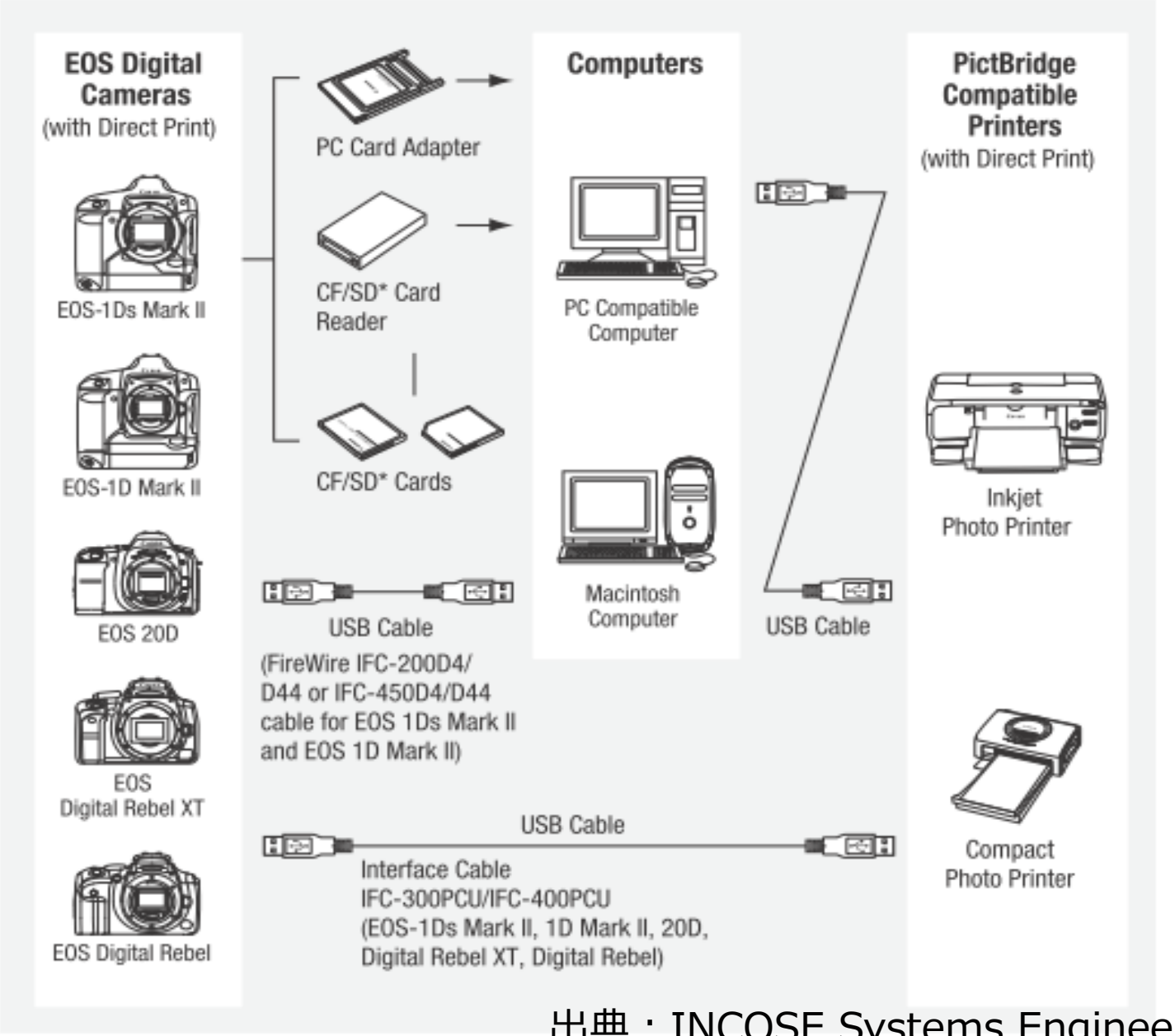
IoT時代の組込みシステムで考慮すべきスコープ
Enterprise Systems Engineering: Seven Samurai



出展：“The Seven Samurai of Systems Engineering Dealing with the Complexity of 7 Interrelated Systems” By James Martin に加筆

Copyright © 2016 IPA, All Rights Reserved

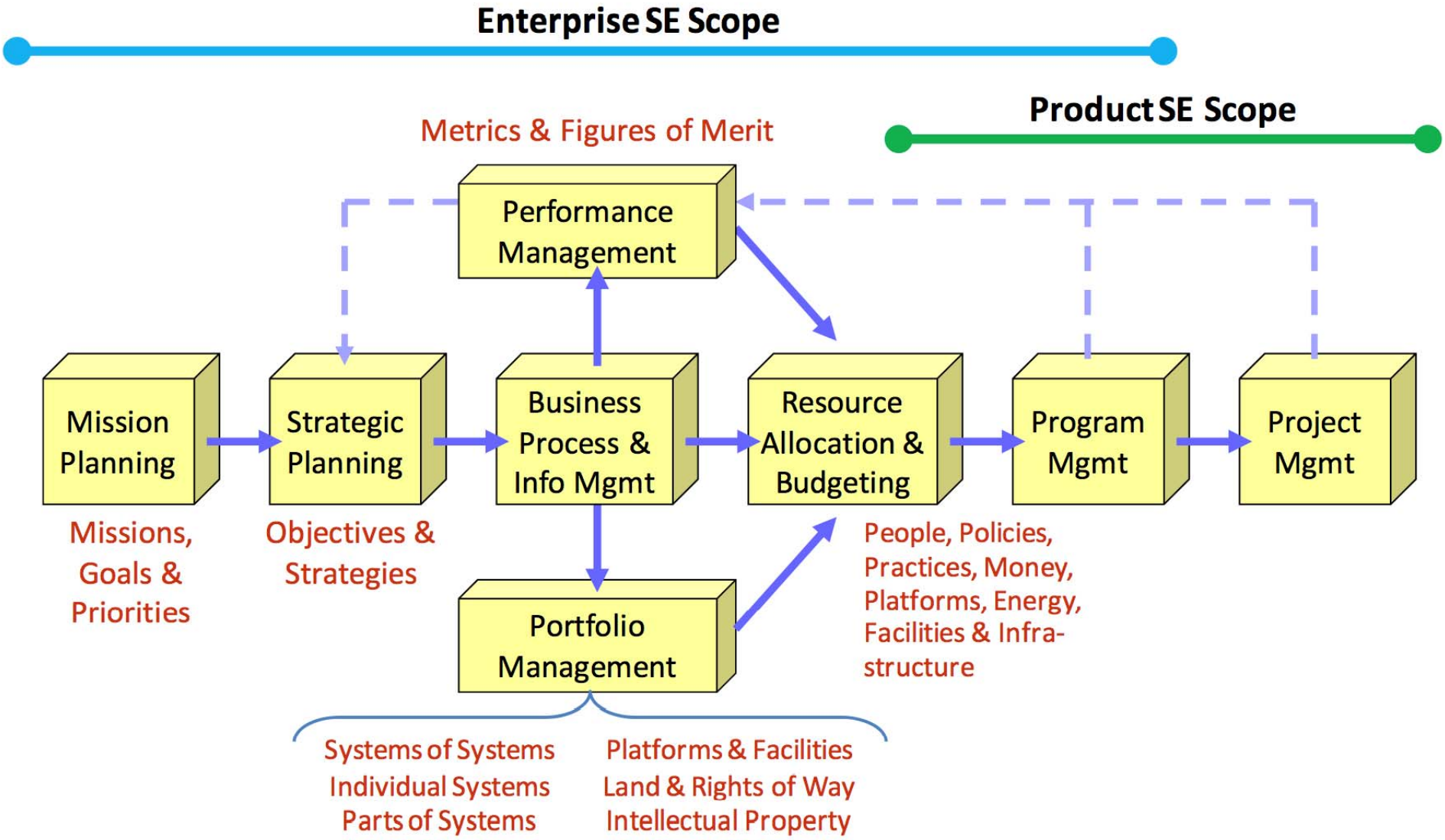
System of Systems



出典：INCOSE Systems Engineering Handbook

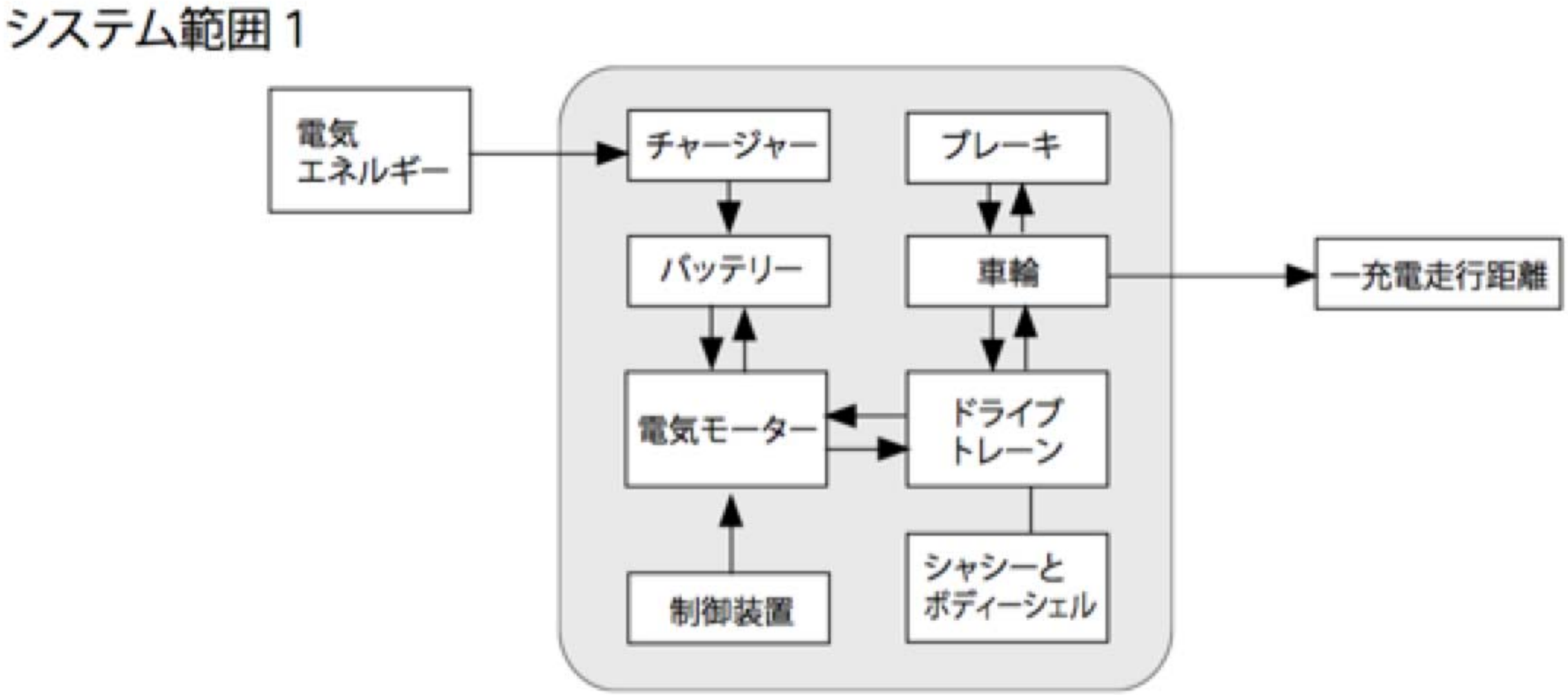
Copyright © 2016 IPA, All Rights Reserved

Enterprise Systems Engineering



出展：”Enterprise Systems Engineering” Edited by George Rebovich, Jr./Brian E. White (2010)

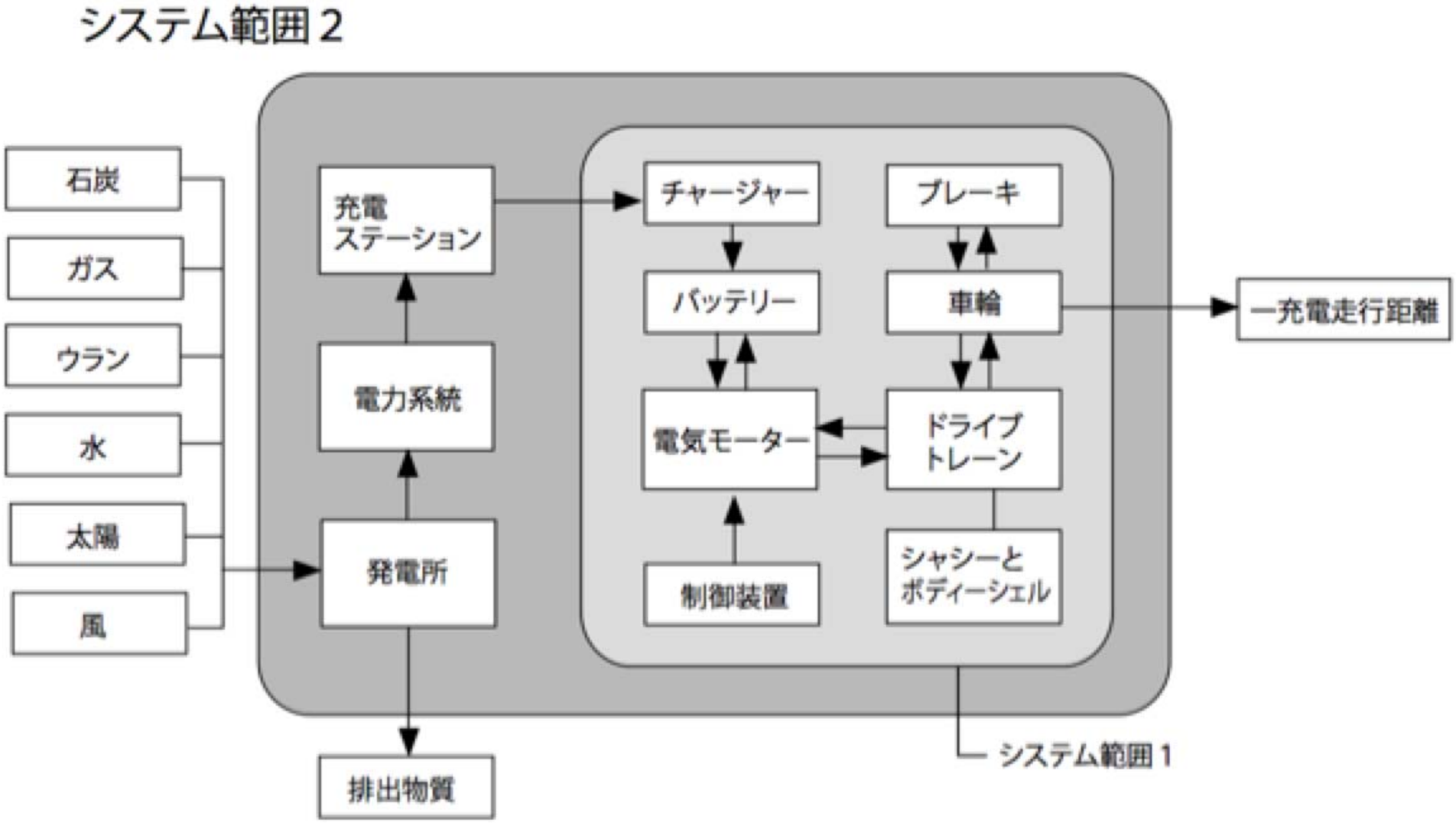
Copyright © 2016 IPA, All Rights Reserved



出典：Engineering Systems

Copyright © 2016 IPA, All Rights Reserved

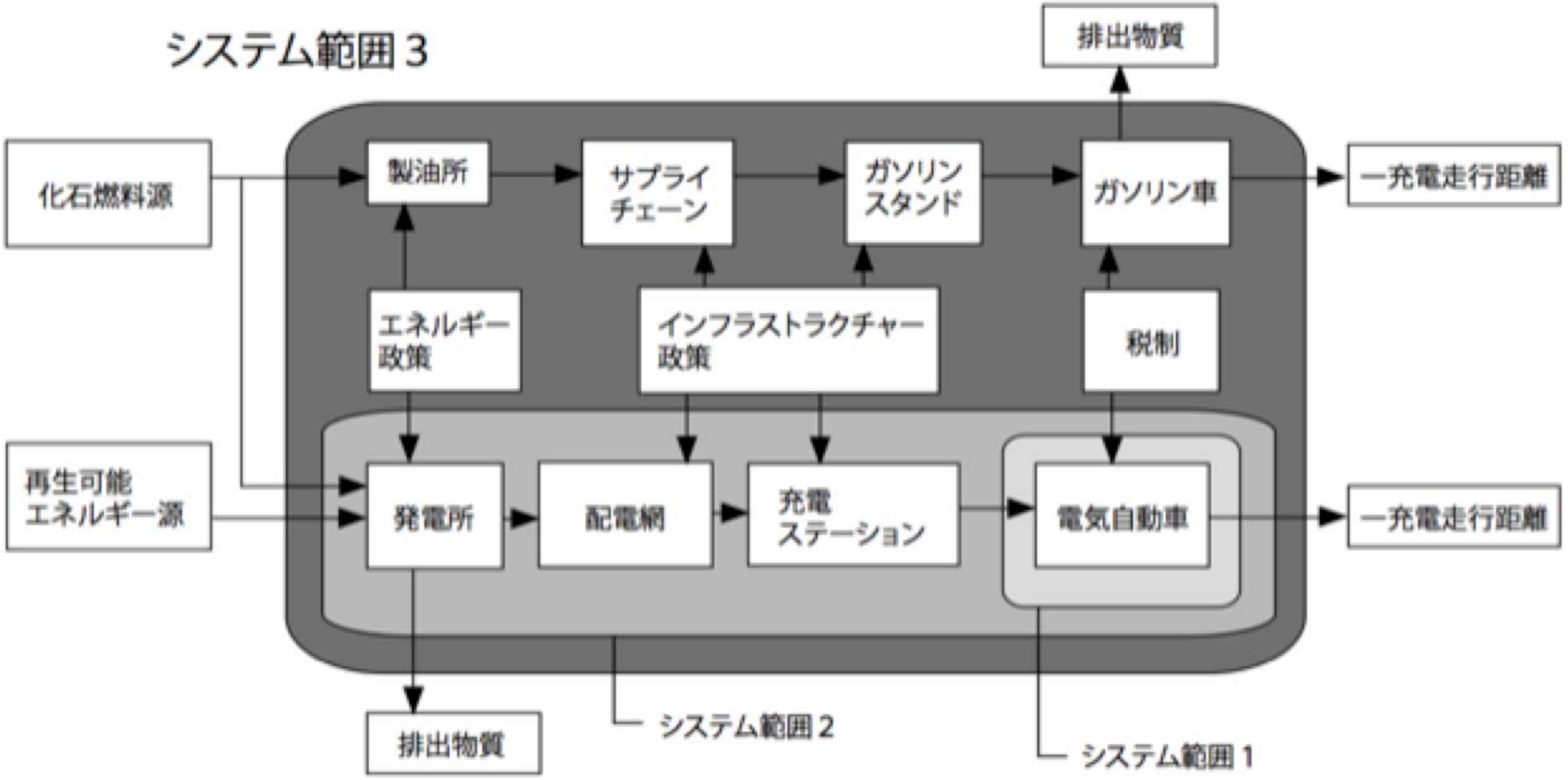
Engineering Systems



出典：Engineering Systems

Copyright © 2016 IPA, All Rights Reserved

Engineering Systems



出典：Engineering Systems

Copyright © 2016 IPA, All Rights Reserved

IoT時代はビジネスチャンス

SEC Software Reliability Enhancement Center

- 世の中は急速にIoTにパラダイムシフト
  - リマンショック後の経済回復フェーズでIoTが浮上地点としてクローズアップ
  - 2020オリンピックを目標に加速する傾向
  - 技術主導だけのIoT拡大は新たな社会課題が噴出
    （無防備なまま発展したインターネットが悪の温床にもなっている事実）
- IoTの進展により産業バリューチェーンが変化
  - 装置（道具）からサービス（道具の活用）へ、サービスからビッグデータ（ノウハウ）へ
- 我が国はIoTの潜在的ポテンシャルは高い
  - 「繋がる」産業の世界トップクラスの企業群が国内に存在
  - 通信技術、組込み技術も世界トップクラスの技術力
  - 我が国産業の国際競争力強化の絶好のチャンス（ただし、ビジネスが弱い）
- 水平分業化が進み機動力のある中小企業が主役になる可能性
  - IoTはそれぞれのシステム階層を担う企業が連携して事業を展開
  - 大手主体の既存の重要インフラに加え、中小主体の新規のIoTインフラが形成
    - センサーネットワークインフラ、ビッグデータインフラ等
  - 大手主体の垂直統合型から中小主体の水平分業型にシフト
    - 大手企業は黎明期の市場規模の小さい事業への参入には消極的
    - 大手企業といえども「Whole Product」の提供が困難に
  - 一方でIoTサプライチェーンの複雑化が潜在リスクを増大

Copyright © 2016 IPA, All Rights Reserved

IoT時代の解決すべき課題

SEC Software Reliability Enhancement Center

- IoTで浮上する新たな課題
  - 業界を跨ったシステムが連携してサービスを提供
    - 異なる文化を持つ業界間で適確な合意形成が非効率的あるいは困難
      （IT関連だけでも、組込み系、モバイル系、クラウド系では文化が異なる）
    - 業界の狭間に潜在的なリスクが残存する可能性
  - 連携する個々のシステムが独立に新陳代謝しながら継続的に進化
    - IoTでは運用開始から高まり続けるリスクモデル
    - 開発期間より遙かに長い運用期間のため活用できない開発者の知見
  - 一つの障害が広範囲に波及・影響するリスク
    - 空間的だけでなく時間的にも広範囲に波及・影響する可能性
      （ビッグデータの不良が世代を超えてリスク拡散する等）
  - 急速に変化する利用形態への対応
    - IoTを前提とした新たな文化と社会モラルとの共存
- IoTの進展で一般国民が置き去りになる可能性大
  - 高齢者やIT弱者もIoTを使わないと生活できない社会に変貌
  - IoT社会に対応した公共サービスが未整備
    - 保健所、消防署等に相当する公共機能
  - IoT社会での生活に必要なIoT教育が不充分
    - イギリスではコンピュータ教育が義務教育でスタート
    - 国内でも、島根県が全中学校でRUBYの教育を実施するなどの例はあるが限定的
    - このままでは日本はIT後進国に（ITの読み書きできない日本人）

Copyright © 2016 IPA, All Rights Reserved

IPA Better Life with IT

ご清聴ありがとうございました

Copyright © 2016 IPA, All Rights Reserved

新試験はじまる！
情報セキュリティマネジメント試験

情報セキュリティの基礎知識から管理能力まで、
組織の情報セキュリティ確保に貢献し、脅威から
継続的に組織を守るための基本的スキルを認定する試験

初回応募者
約2万3千人！！

◆受験をお勧めする方◆

- 個人情報を扱う全ての方
- 業務部門・管理部門で
  情報管理を担当する全ての方

◆28年度秋期試験実施時期◆

- **実施日**　2016年10月16日（日）
- **申込受付**　2016年7月11日（月）から

ITパスポート試験

あなたのＩＴ力を証明する国家試験

ITパスポート公式キャラクター
上峰亜衣（うえみねあい）

【プロフィール：マンガ】 https://www3.jitec.ipa.go.jp/JitesCbt/html/uemine/profile.html

「iパス」は、ITを利活用するすべての社会人・学生が備えておくべき
ITに関する基礎的な知識が証明できる国家試験です。

IPA
Better Life
with IT