IPA
Information-technology
Promotion
Agency, Japan

つながる世界のセキュリティ設計実践に向けて

2017年6月20日

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
中尾　昌善

便利になりつつあるIoT時代（その１）

バルセロナ市の公共IoT（スマートパーキング）の例

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 8.9 Picture of the selected Smart Parking test facility

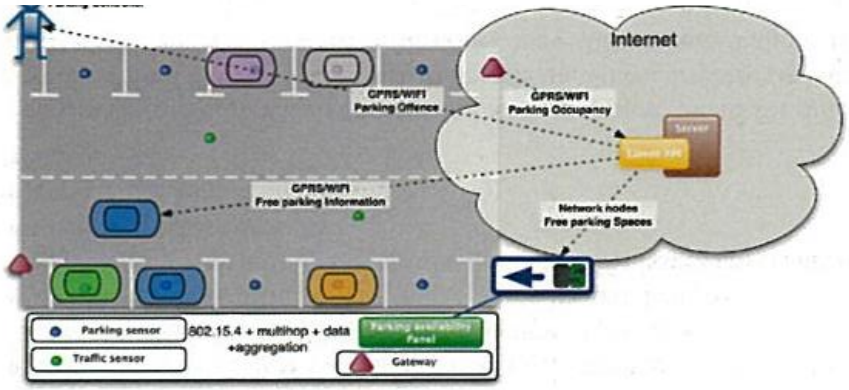


Figure 8.1 Architecture of the parking space availability control service

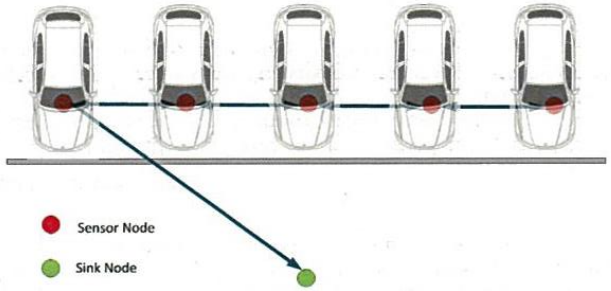


Figure 8.10 Configuration of the network topology

出典：Internet of Things - From Research and Innovation to Market Deployment

便利になりつつあるIoT時代（その２）

JR東日本「スマートメンテナンス」の例

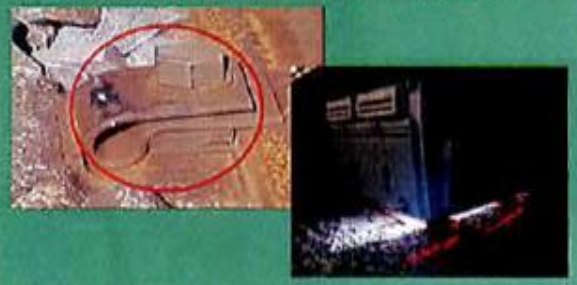
センサ・ビックデータを活用した保守コストの大幅削減
～　時間計画保全から状況監視保全へ　～

○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。

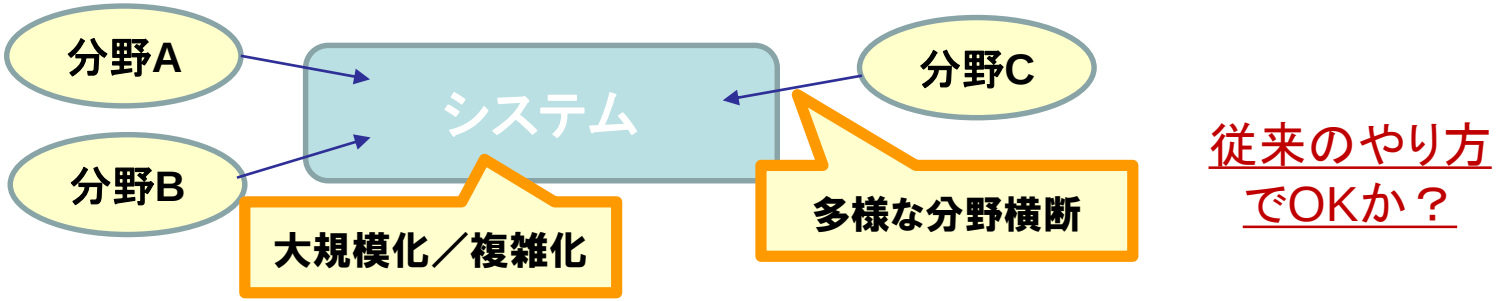
「スマートメンテナンス」機能搭載を予定している
JR山手線の新型車両「E235系」

出典：JR東日本WEB、ITproニュース2014.8.26記事

一方で、IoT時代には、様々な課題が存在

1）これまで想定しなかった機器類のつながりが発生し、リスクが増大

2）システムが大規模化／複雑化／分野横断化し、開発失敗の懸念



製品やシステム開発時の「安全・安心」への対策が急務！

IoT時代の安全・安心のための高信頼化

IoT製品やシステムの高信頼化

「つながり」によって発生するリスクを回避するための製品・システム開発

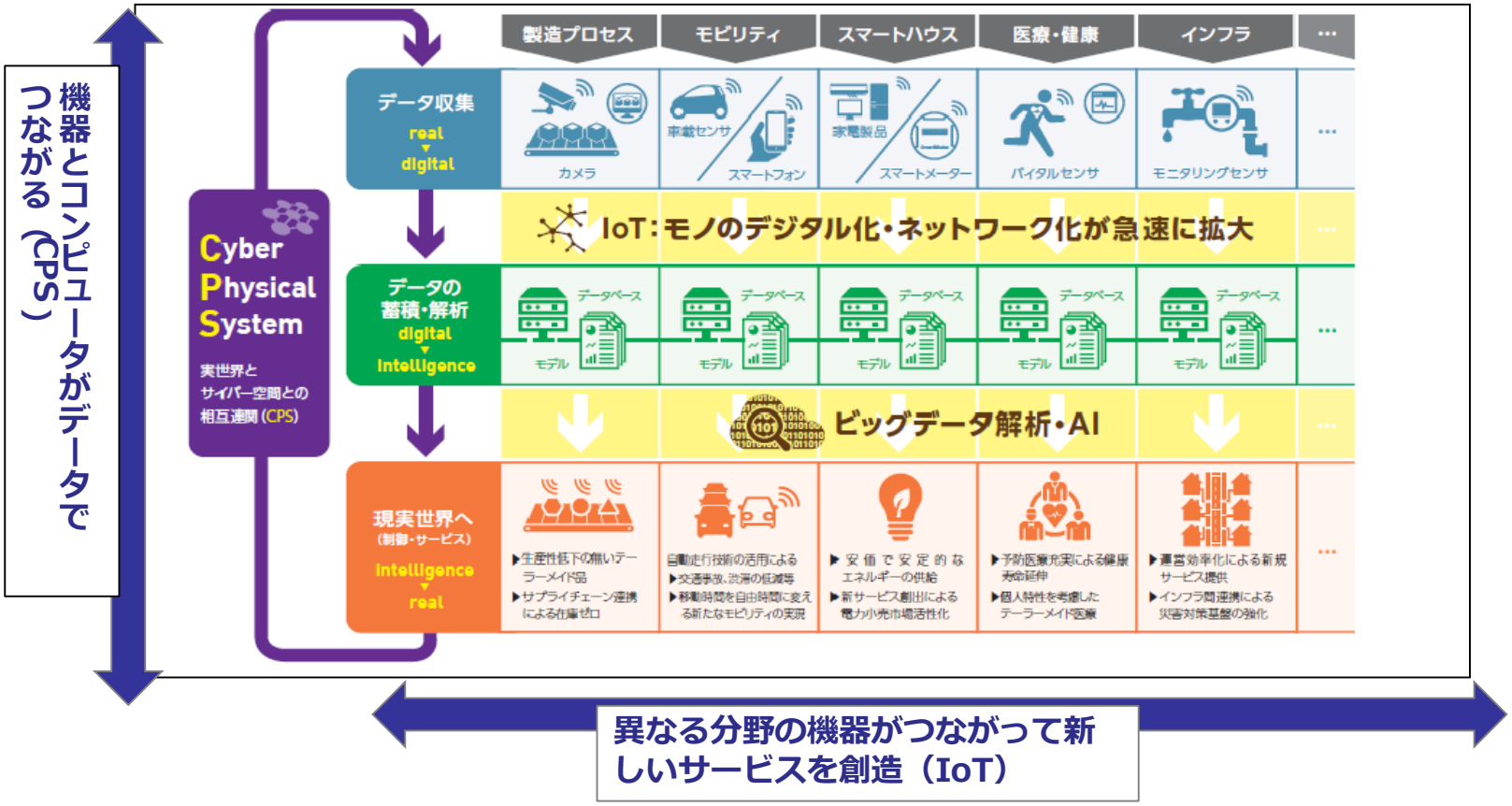
Ⅰ）「つながる世界の開発指針」をベースとした高信頼化

大規模・複雑化するシステムの課題を解決するための開発方法のパラダイムシフト

Ⅱ）　新たな開発アプローチ

1）．今後の「つながる世界」

SECでは、「つながる世界」≒「IoT時代」という意味で、この用語を用いています。



「Cyber Physical “society”（CPS（超情報化）社会）の概念図 【出典】平成27年4月　産業構造審議会 商務流通情報分科会 情報経済小委員会 中間とりまとめ」を元に追記

課題認識の典型例：接続先は信頼できる？

設計要件が異なる際に想定されるリスク

- 持ち主以外からの接続による車の盗難
- 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
- 脆弱性がある側の製品や機器への不正アクセスにより、相手側の製品や機器に保存されている情報が盗難

等

IoT時代の安全安心への危惧

注）安全安心・・・ここでは、セーフティ・セキュリティ・リライアビリティを表す用語として用いています。

「つながる世界の開発指針」の策定

IoT時代には、これまで想定しなかった機器類のつながりが発生し、リスクが増大

開発時の拠り所が欲しいという産業界の要請

「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（PDF版）
http://www.ipa.go.jp/sec/reports/20160324.html

１７個の指針

◆ 製品の開発ライフサイクル全体において考慮すべき17の指針を策定

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

※指針は、ポイント、解説、対策例を記述

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

個別企業における開発指針の適用例

組込み実態調査（５月公開）によれば、既に約20%の企業で活用、または活用予定

チェックリストにより、各社で指針適用の確認が可能

【開発指針の活用事例】

- （１）IoT製品開発時の留意点として活用
- （２）受発注の要件確認に活用
  （英語版も公開しているので、オフショアにも適用可能）
- （３）考慮結果を取組みのエビデンスとして活用
- （４）IoT製品の安全性を説明する営業ツールとして活用

機能レベルにまで踏み込んだ手引き

（１）「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】を作成（2017年5月８日公開）

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とクラウド・フォグ・エッジ等の機能配置を考慮し網羅的にイメージ

③IoTの分野間連携のユースケースと、リスクや脅威、機能定義や機能配置の具体例

IoT高信頼化要件・機能

IoT高信頼化要件		IoT高信頼化を実現するための機能要件	対応するIoT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	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
		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	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
		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
		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	異常発生を監視・通知できる	監視機能、状態可視化機能、
		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	構成の把握ができる	構成情報管理機能
		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
		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	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
		データ消去ができる	消去機能

例１ ［開始］導入時や利用開始時に安全安心が確認できる

- 初期設定の不備をなくすとともに、許可された者か・アクセス可能なデバイスかなどの設定や確認を行う

		1 初期設定機能	2 設定情報確認機能	3 認証機能	4 アクセス制御機能
【機能要件1】初期設定が適切に行われ、その確認ができる		✔	✔		
	安全安心に係る初期設定が適切に行われる				
	初期設定が適切であることを確認できる				
【機能要件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				✔	✔
	接続されるときに本人や正しい機器であるかを確認できる				
	設定された情報にもとづき利用の許可/制限ができる				
	相互の信用度を確認して接続の可否判断ができる				

例２［予防］稼働中の異常発生を未然に防止できる

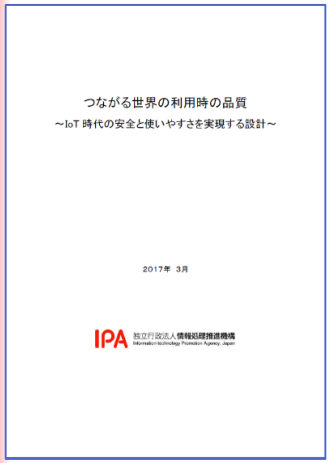
- 異常の発生を予知や、守るべきもの保護や、問題の事前対処を行う

	4 アクセス制御機能	5 ログ収集機能	6 時刻同期機能	7 予兆機能	8 診断機能	9 ウイルス対策機能	10 暗号化機能	11 リモートアップデート機能
【機能要件3】異常の予兆を把握できる		✔	✔	✔	✔	✔		
異常の発生を予測し、それを通知する								
ハードウェアの正常動作の確認やウイルス対策を行う								
【機能要件4】守るべき機能・資産を保護できる	✔	✔	✔				✔	
守るべきものを特定し保護する								
保護状態が維持できているかを確認する								
【機能要件5】異常発生に備えて事前に対処できる								✔
遠隔で改修できる								

つながる世界の利用時の品質

つながる世界の利用時の品質～IoT時代の安全と使いやすさを実現する設計～

報告書公開URL：https://www.ipa.go.jp/sec/reports/20170330.html

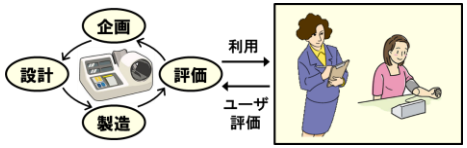


利用時の品質向上のための15の視点

区分		視点
組織文化	1	つながる世界の利用時の品質を意識する
	2	他部門と連携して取り組む文化を作る
	3	自社や顧客の責任者の意識を変える
	4	利用時の品質向上に関わる人材を育成する
把握・分析	5	ユーザの特性や経験、文化、利用環境を考慮する
	6	ユーザ経験を収集・分析・評価する
	7	間接・受動的ユーザやプライバシーにも配慮する
	8	利用状況や利用環境の変化の影響を考慮する
設計	9	企画・設計段階からユーザを巻き込む
	10	ユーザを安全な操作に導く設計をする
	11	第三者に機能や情報を使わせない設計をする
	12	操作結果やメッセージを確実に伝える設計をする
保守・運用	13	ユーザや関係者からフィードバックを得る仕組みを作る
	14	知見を開発時及び出荷後の利用時の品質向上に活用する
	15	つながるリスクの周知と安全設定の仕組みを作る

組織文化の醸成

ユーザ経験の**把握・分析**

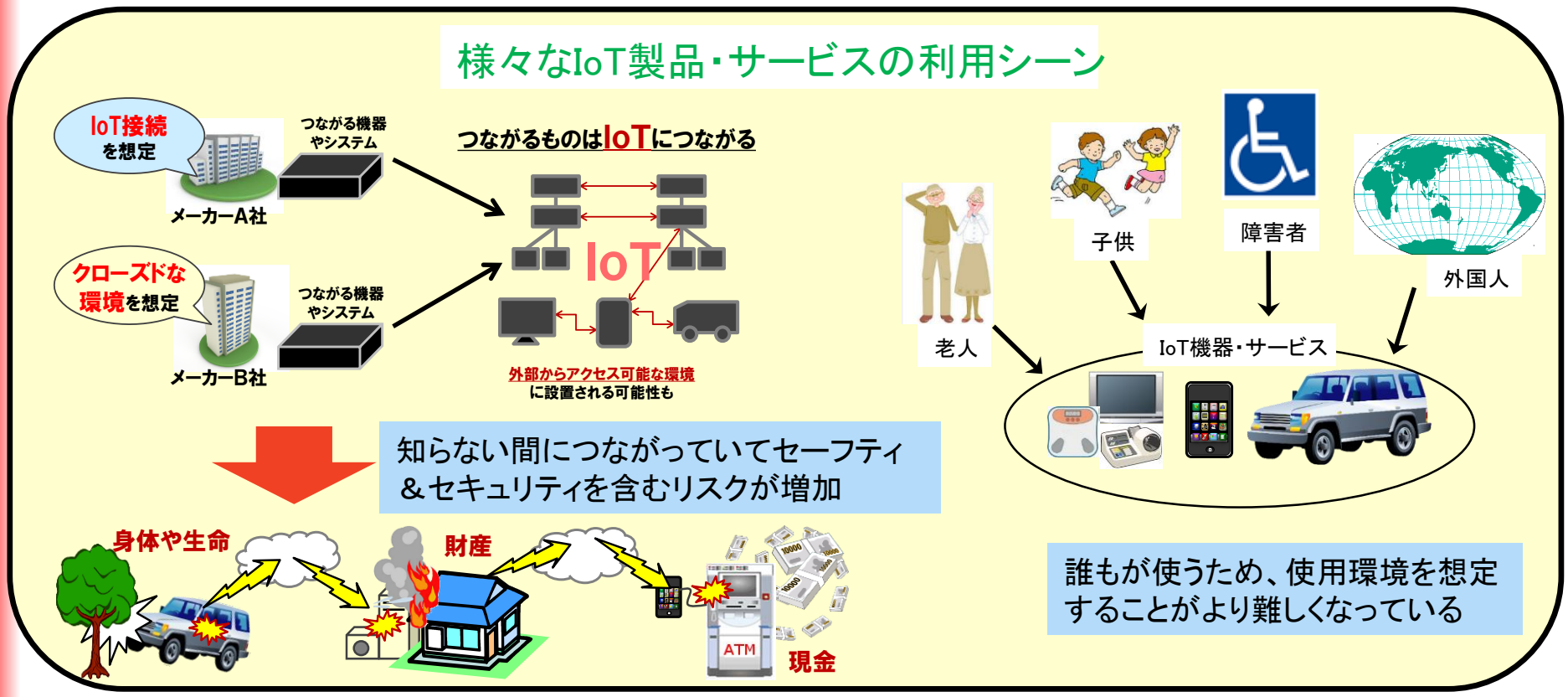


ユーザを巻き込んだ**設計**

知見をまとめる**保守・運用**

利用時の品質に着目した背景

これからのIoT製品・サービスは多種、多様な形で利用されることが想定され、
利用者の目的や特性および利用環境を考慮した高い信頼性を確保できる
（＝「利用時の品質」を考慮した）製品開発が重要。



【背景】IoT時代のシステム課題

ビジネスチャンスの裏には経営リスクも！

従来は想定されなかったようなモノ・コトのつながり

隣接する分野の事業への進出

つながる相手への迷惑、相手からの迷惑

単一分野でのビジネスルールが通用しない

想定リスク

新サービスが生まれることによるビジネス環境の変化

考慮すべき条件の拡大

現ビジネス領域の衰退

考慮もれによる失敗（不備、遅延、事故）

転ばぬ先の杖（新たなアプローチ）の導入が必要

システム開発における課題事例（１）

- 鉄道・列車制御システムの更新とサービス継続

  混雑緩和の社会要請の強まりに応え、運転本数を増加できる新しい列車制御システムを開発した事例

  – 開発上の課題

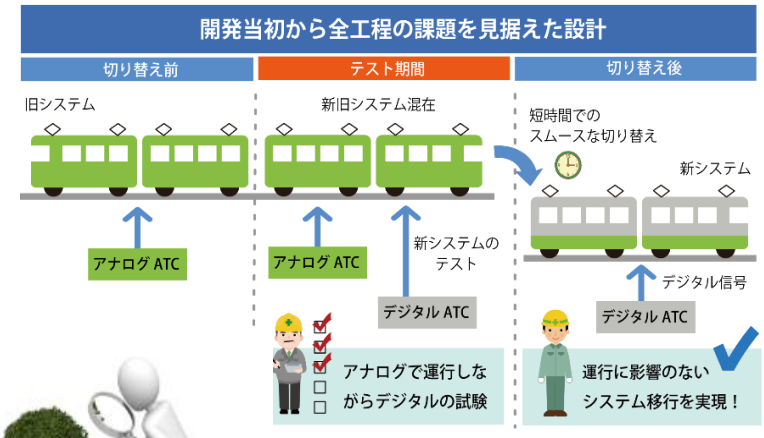
    現行システムに影響しない新システムの検証方法、運行を維持しながらの新システムへの迅速な切替え

  – 上記の解決策

    開発当初から全工程の課題を見据えて（時間軸を俯瞰）、システム移行を考慮して設計

解決のポイント

目的指向と全体俯瞰



出典：SEC Journal 35号（IPA）アシュアランス技術を用いた鉄道信号の革新

システム開発における課題事例（２）

- 国境にまたがる最大の複合構造物（オーレスン橋）の建設
  デンマーク・スウェーデン国境をまたぎ、車道と鉄道を備えた世界最大の斜張橋(7.85km)でもあるオーレスン橋建設の事例
  - 開発上の課題
    多岐にわたる専門領域（橋梁土木、道路交通、環境保全、等）、両国の規制・基準の違い／鉄道方式の違い、右側/左側通行、電力供給方式、環境問題　等
  - 上記の解決策
    多様な専門分野を統合した
    構想段階における綿密な計画

解決のポイント

多様な専門分野を統合

出典：SEBoK(Guide to the Systems Engineering Body of Knowledge，

前述の課題解決に寄与したアプローチ

解決ポイント➡システムズエンジニアリング

①目的指向と全体俯瞰

- 解決策を考える前に本来の目的を明確にし、常に目的を意識しながら考えます。
- 視点と視野を変えながら俯瞰して捉えます。視点としては、時間的視点、空間的視点、意味的視点があります。

  時間的俯瞰の例：
  初期から利用終了後の廃棄まで、さらに
  世代交代までのライフサイクル全体

②多様な専門分野を統合

- 多様な分野（技術、事業、領域、環境、文化、社会など）の知見を統合します。

③抽象化・モデル化

- 抽象化の視点を柔軟に設定し、多視点から対象を構造化し、システムに関する様々なネットワークを通じて、システムを明らかにします。
- モデルを利用することによって異なる分野の人たちの間での概念共有、情報共有による共通理解の促進を図ります。

④反復による発見と進化

- 適切に再評価とフィードバックを反復して、新たな解決方法を発見し、段階的に明確化・進化させます。

出典：「経営者のためのシステムズエンジニアリングの薦め」(IPA/SEC)

システムズエンジニアリングとは？

「システムを成功させるための複数の専門分野にまたがるアプローチと手段である」 JCOSE(Japan Council on Systems Engineering)

ここでいう「システム」は、コンピュータシステムにとどまらず、機械、電気機器、人間系（操作者）、環境など広い意味を表す。

航空･宇宙領域で確立した企画･開発のアプローチを汎用的に体系化したもの　⇒欧米を中心に発展

システムズエンジニアリングを適用しない場合に比べて、最適に適用した場合のコスト、納期は、
凡そ70%、55%

ご清聴ありがとうございました。