FUJITSU
shaping tomorrow with you

【SPI Japan 2019発表資料】

新領域の製品・サービスの利用時に起こり得る品質問題解析へのSTAMP/STPAの応用

～利用時品質の評価技術の体系化と新分野での実践～

富士通クオリティ・ラボ株式会社 プロセスコンサル事業部
高橋　和博

株式会社富士通コンピュータテクノロジーズ　ＴＭＰ事業部
小松　隆

自己紹介

FUJITSU

富士通クオリティ・ラボ株式会社 プロセスコンサル事業部

プロフェッショナル・クオリティ・エンジニア

高橋 和博（たかはし かずひろ）

- **品質改善支援、プロセス構築、品質セミナー講師**
- Provisional Assessor Automotive SPICE®
- QMS(ISO9001)審査員補(JRCA認定)
- IATF16949内部監査員
- 横浜国立大学「創造的な技術者リーダー育成プログラム」に参加
- 富士通グループ　品質保証技術コミュニティ　利用時品質WG　など

品質に厳しい航空機、スマートフォン、自動車搭載からICT分野まで、幅広い製品・サービスの開発、品質を担当

現在は、**人間の行動特性と　品質保証技術**　を分かりやすく融合し、お客様のニーズに応え　ビジネス成功へ導く支援をしています。

Copyright 2019 FUJITSU QUALITY LABORATORY LIMITED
Copyright 2019 FUJITSU COMPUTER TECHNOLOGIES LIMITED

富士通のプロフェッショナルエンジニア制度

PPE（Professional Product Engineer）

■PPE認定をとおして、プロフェッショナルエンジニアが、組織の枠に捉われず、技術面からビジネスに貢献することを目指す

■コミュニティという部門横断的にPPE同士が集まることができる場を用意し、技術貢献活動を進める体制

PPE　品質保証技術コミュニティ　利用時品質WG

■新領域の製品・サービスの品質リスクの分析手法検討

■利用時品質を阻害する新しいタイプの損害やストレスの発生防止

Copyright 2019 FUJITSU QUALITY LABORATORY LIMITED
Copyright 2019 FUJITSU COMPUTER TECHNOLOGIES LIMITED

目次

FUJITSU

1 取り巻く環境／新領域の製品・サービス開発の課題

2 失敗からの気づき／改善したいこと／本提案の着想

3 本当に STAMP/STPA は使えるのか？

4 改善のための施策

5 まとめ

6 今後の取り組み

Copyright 2019 FUJITSU QUALITY LABORATORY LIMITED
Copyright 2019 FUJITSU COMPUTER TECHNOLOGIES LIMITED

1 取り巻く環境／新領域の製品・サービス開発の課題

2 失敗からの気づき／改善したいこと／本提案の着想

3 本当に STAMP/STPA は使えるのか？

4 改善のための施策

5 まとめ

6 今後の取り組み

Copyright 2019 FUJITSU QUALITY LABORATORY LIMITED
Copyright 2019 FUJITSU COMPUTER TECHNOLOGIES LIMITED

取り巻く環境

IoT・ビッグデータ・AI……など、新しいテクノロジーが次々と登場し、
これらを使ったサービスや機器の進化には目覚ましいものがある。

IoT・ビッグデータ・AI等の進化したICTの利活用が創造する未来は、
潜在需要を喚起する新商品・サービスの開発・提供など
様々なイノベーションの実現を可能にするとみられている。

IoT・ビッグデータ・AI～ネットワークとデータが創造する新たな価値～　総務省，平成28年版　情報通信白書

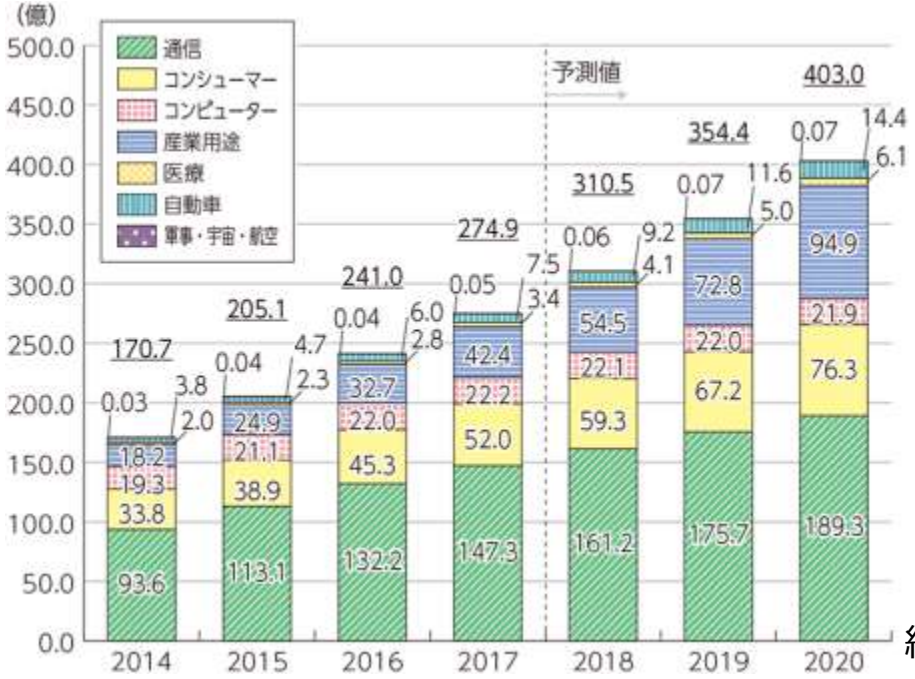
Copyright 2019 FUJITSU QUALITY LABORATORY LIMITED
Copyright 2019 FUJITSU COMPUTER TECHNOLOGIES LIMITED

新領域の製品・サービス開発の課題

FUJITSU

- 既存の解析手法やテストで保証しきれず品質問題に至る可能性
  - 従来のシステムよりも不確実性が高く流動的
  - 人間や環境、他システムとの相互作用でアクシデント発生

世界では、AI・IoTの普及が進み、IoTデバイス数は2017年には約270億、2020年には約400億の予測



総務省, 平成30年版　情報通信白書

Copyright 2019 FUJITSU QUALITY LABORATORY LIMITED
Copyright 2019 FUJITSU COMPUTER TECHNOLOGIES LIMITED

新しいタイプの損害やストレス

FUJITSU

- 従来の製品・サービスは、基本的に以下の特徴を持っていた
  - 製品・サービスに対して何を入力しているのかが明確
  - 入力に対する出力の期待値が明確
- 昨今の製品・サービスは「人間的」もしくは「人間味がある」ことを要求されるケースが増えており、以下のような特徴が明示的/暗黙的な要求となってきている
  - 製品・サービスに対する入力操作や仕組みを利用者に意識させない
  - 入力に対して出力を求めるための論理が仕様化できない(AIや機械学習などによって実現する)

利用者にとって、入力や出力が曖昧で論理が明確になっていないことで、新しいタイプの損害やストレスが世の中で発生しはじめている

Copyright 2019 FUJITSU QUALITY LABORATORY LIMITED
Copyright 2019 FUJITSU COMPUTER TECHNOLOGIES LIMITED

FUJITSU

1 取り巻く環境／新領域の製品・サービス開発の課題

2 失敗からの気づき／改善したいこと／本提案の着想

3 本当に STAMP/STPA は使えるのか？

4 改善のための施策

5 まとめ

6 今後の取り組み

Copyright 2019 FUJITSU QUALITY LABORATORY LIMITED
Copyright 2019 FUJITSU COMPUTER TECHNOLOGIES LIMITED

失敗からの気づき

FUJITSU

ドライバーが運転中に身に着け生体信号をモニタするIoTデバイス（新領域の製品）で、

装着方法の改造によりケーブル断線不具合が市場で多発

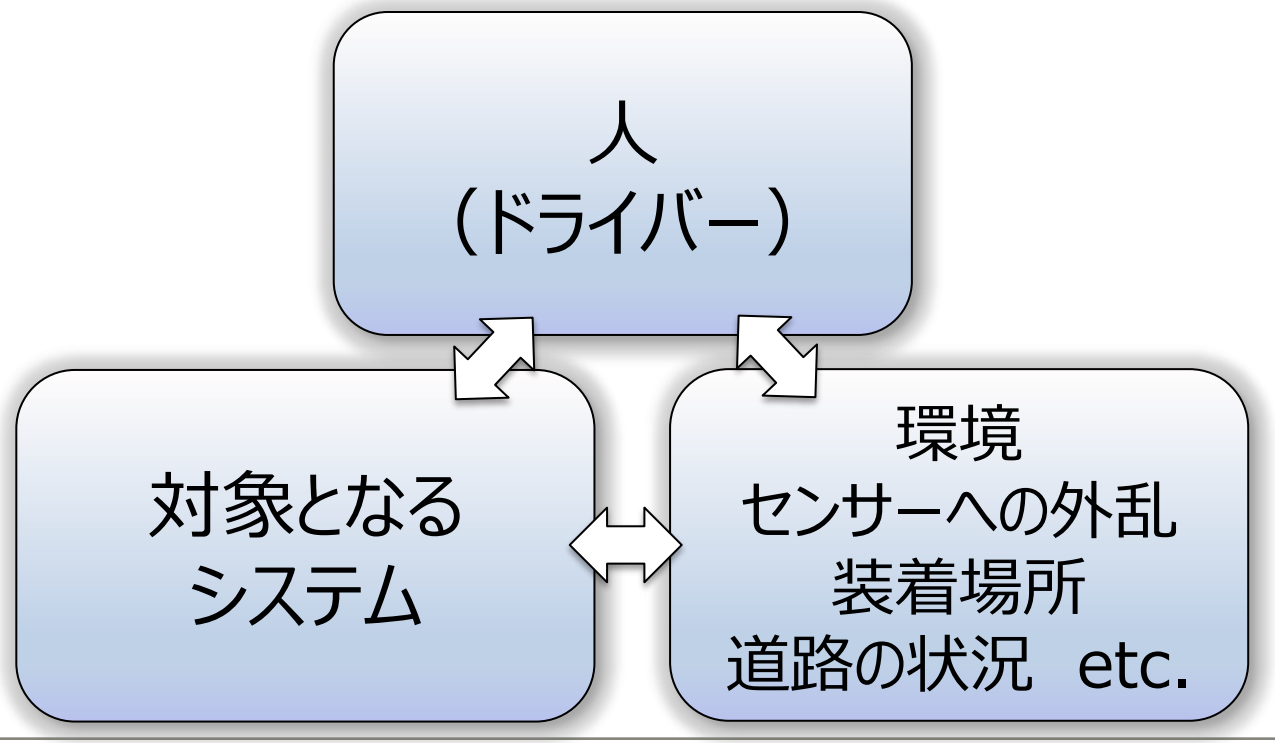
Copyright 2019 FUJITSU QUALITY LABORATORY LIMITED
Copyright 2019 FUJITSU COMPUTER TECHNOLOGIES LIMITED

失敗からの気づき

FUJITSU

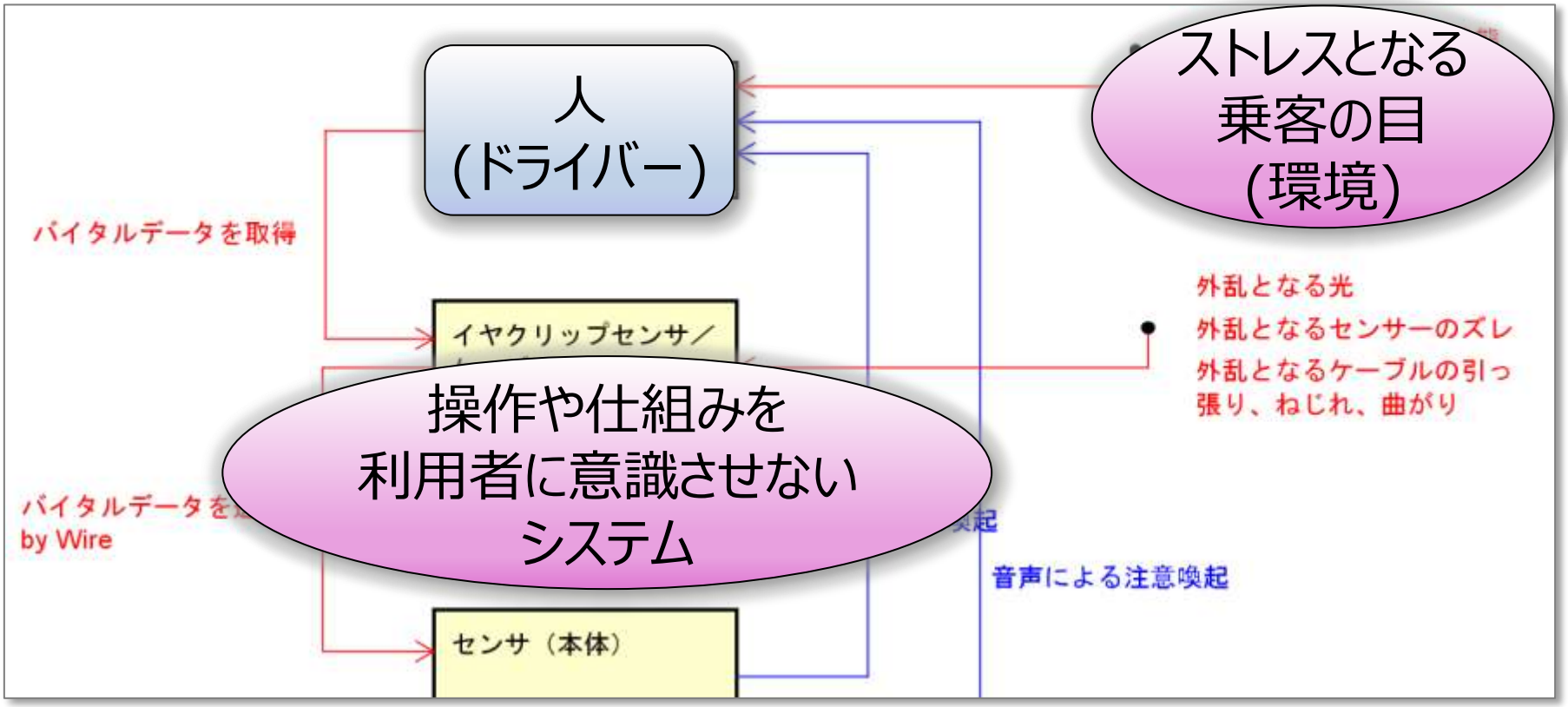
リスク分析も検証・テストもやったにもかかわらず、市場で不具合が起こってしまったのはなぜか？

人を中心に置いて、対象となるシステムや環境の相互作用に着目した新しい解析手法STAMPで原因を分析してみた



Copyright 2019 FUJITSU QUALITY LABORATORY LIMITED
Copyright 2019 FUJITSU COMPUTER TECHNOLOGIES LIMITED

STAMP／STPAによる原因分析



装置の特性やドライバーの心理から不具合に至るシナリオを導出できた

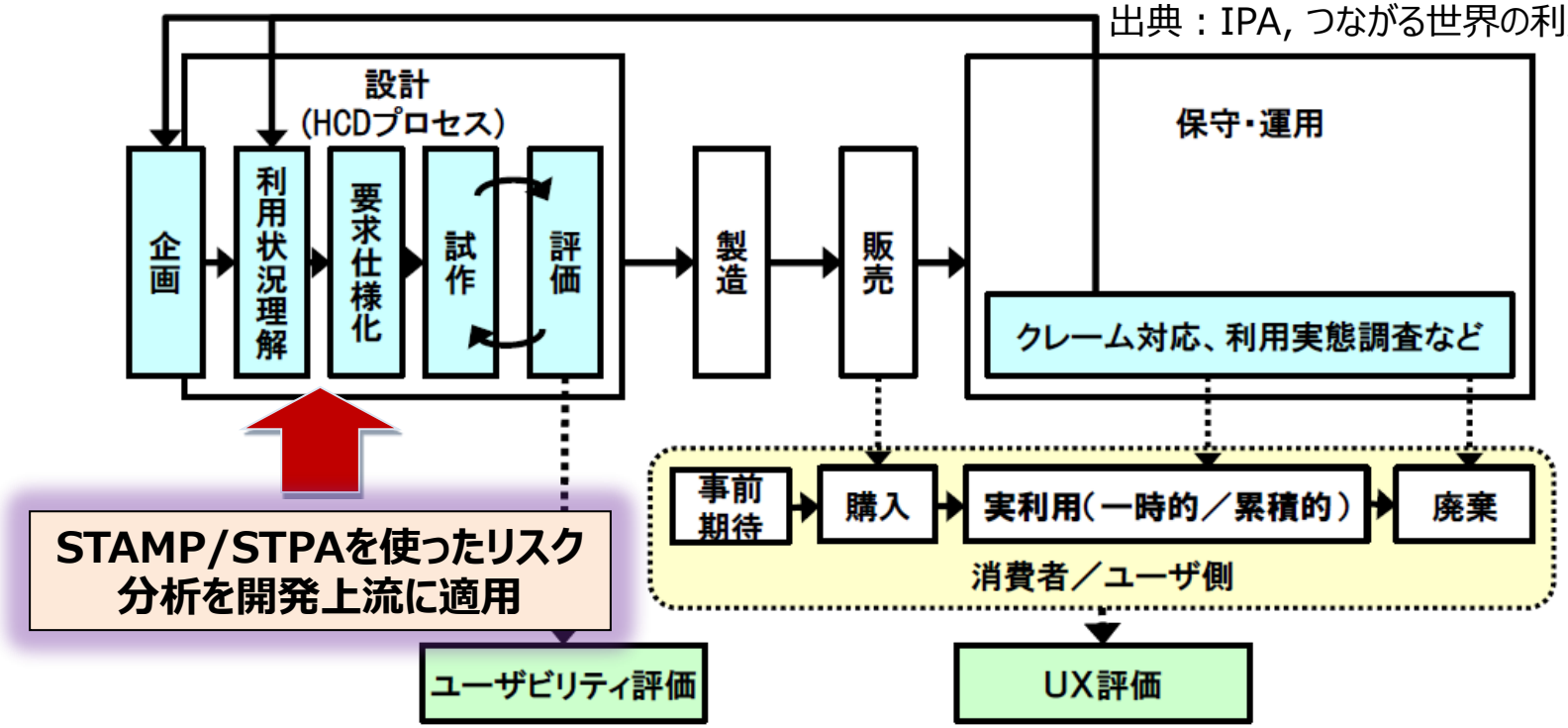
ドライバーにとって、入力や出力が曖昧で仕組みが不明確なモノを身に着けており、ケーブルの長さが煩わしく且つ乗客の目が気になり、ケーブルを “折り畳んで” 継続使用した結果、断線に至った

Copyright 2019 FUJITSU QUALITY LABORATORY LIMITED
Copyright 2019 FUJITSU COMPUTER TECHNOLOGIES LIMITED

本提案の着想

FUJITSU

出典：IPA, つながる世界の利用時の品質



人や環境、他システムとの相互作用に着目し
開発上流から適用可能と言われている
STAMP/STPA が
新しいタイプの損害やストレスの抽出に使えないか

Copyright 2019 FUJITSU QUALITY LABORATORY LIMITED
Copyright 2019 FUJITSU COMPUTER TECHNOLOGIES LIMITED

改善したいこと

FUJITSU

■ 品質が設計・テストで保証しきれず品質問題に至る可能性

- 新しいタイプの損害やストレスでは、経験や実績が十分活かされない
- 装置主体の従来の開発プロセスでは抜け漏れ防止に対応しきれない（FMEA, 評価・検証, レビュー, ユーザビリティテストなど）

新しいタイプの損害やストレスを未然防止するため、開発上流でSTAMP/STPAを使って抽出できるようにしたい

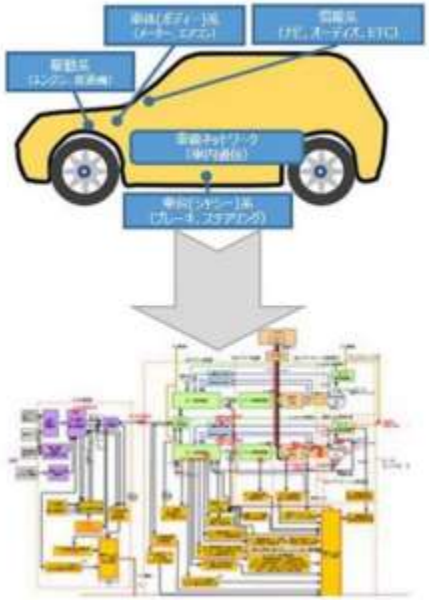
Copyright 2019 FUJITSU QUALITY LABORATORY LIMITED
Copyright 2019 FUJITSU COMPUTER TECHNOLOGIES LIMITED

STAMP/STPA とは

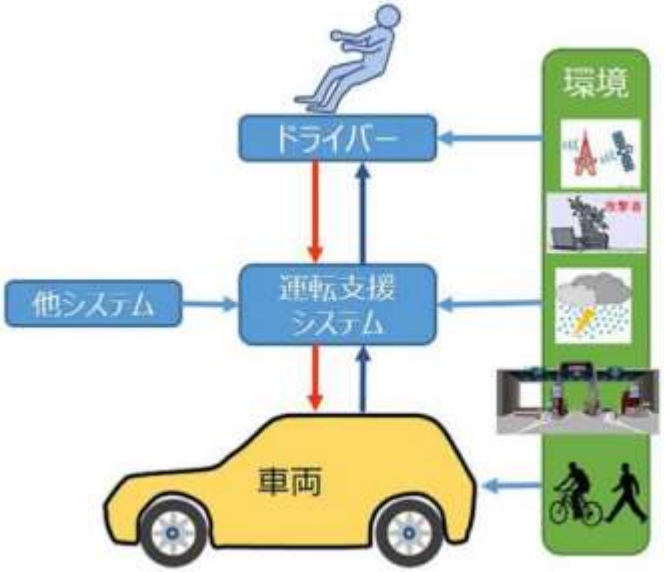
FUJITSU

- **システム思考に基づく アクシデント モデルおよびプロセス:**
  STAMP (Systems-Theoretic Accident Model and Processes)
- **STAMPに基づくハザード解析手法:**
  STPA (STAMP-Based Process Analysis)

従来は、コンポーネントを組み合わせた“システム”の分析を徹底的に行っていた



対象となるシステムだけではなく、**人間や環境、その他のシステムとの相互作用に着目**



アクシデント：望んでもいないし、想定もしていない損失（事象）
ハザード　　：条件によってアクシデントにつながるようなシステムの状態

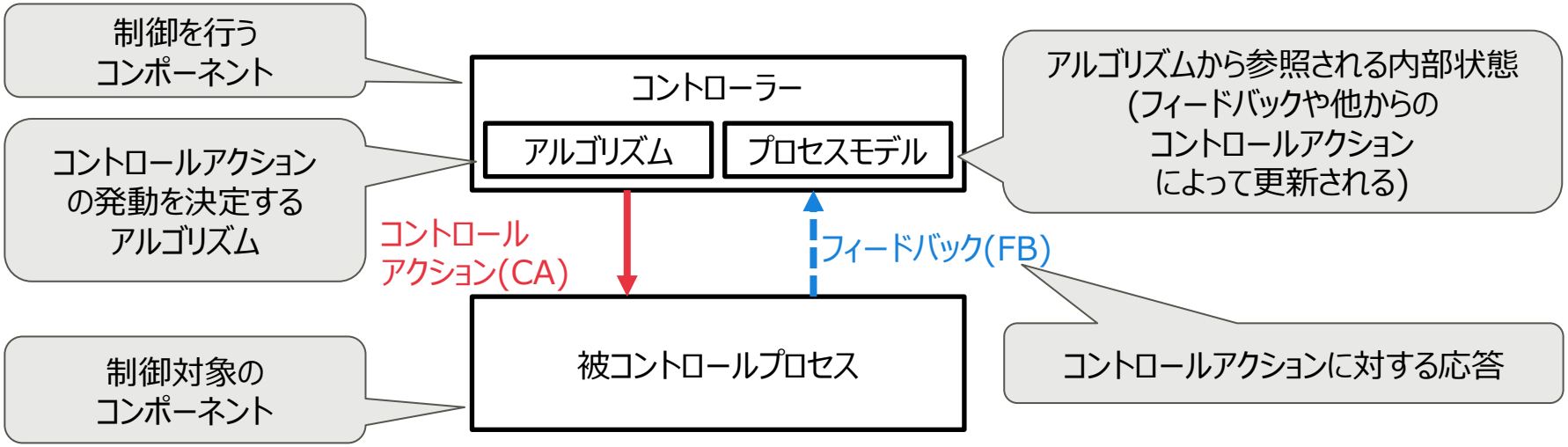
出典：IPA, はじめてのSTAMP/STPA

Copyright 2019 FUJITSU QUALITY LABORATORY LIMITED
Copyright 2019 FUJITSU COMPUTER TECHNOLOGIES LIMITED

STAMPでは構成要素の相互作用に注目する

FUJITSU

STAMPでは、システムの構成要素ではなく、制御する側(コントローラー)と制御される側(被コントロールプロセス)の間の相互作用に着目する



Copyright 2019 FUJITSU QUALITY LABORATORY LIMITED
Copyright 2019 FUJITSU COMPUTER TECHNOLOGIES LIMITED

STAMP/STPAによる分析手順の概観

FUJITSU

- アクシデント、ハザード、安全制約の識別

  どんなアクシデントを防ぎたいかを明らかにする

  （分析の目的を定める）

- 制御構造図の構築

  コンポーネント間の制御の関係を絵にかく

- 非安全なコントロールアクション(UCA) の抽出

  ガイドワードを使って ハザードが起きるシナリオ (UCA) をラフに分析する

  - 与えられないとハザード
  - 与えられるとハザード
  - 早すぎ、遅すぎ、誤順序ならハザード
  - 早すぎる停止、停止まで長すぎるとハザード

- ハザード誘発要因(HCF) の特定

  ヒントワードを使ってUCAに繋がる潜在原因を識別する

UCA: Unsafe Control Action
HCF: Hazard Causal Factor

Copyright 2019 FUJITSU QUALITY LABORATORY LIMITED
Copyright 2019 FUJITSU COMPUTER TECHNOLOGIES LIMITED

FUJITSU

1 取り巻く環境／新領域の製品・サービス開発の課題

2 失敗からの気づき／改善したいこと／本提案の着想

3 本当に STAMP/STPA は使えるのか？

4 改善のための施策

5 まとめ

6 今後の取り組み

Copyright 2019 FUJITSU QUALITY LABORATORY LIMITED
Copyright 2019 FUJITSU COMPUTER TECHNOLOGIES LIMITED

FUJITSU

本当に STAMP/STPA は使えるのか？

人とモノがつながる身近な事例で試行

（例）

- 自転車
- 電車のドアの開閉システム
- 回転ドア
- グループウェア・サービス

Copyright 2019 FUJITSU QUALITY LABORATORY LIMITED
Copyright 2019 FUJITSU COMPUTER TECHNOLOGIES LIMITED

STAMP/STPA 適用の仮説-1

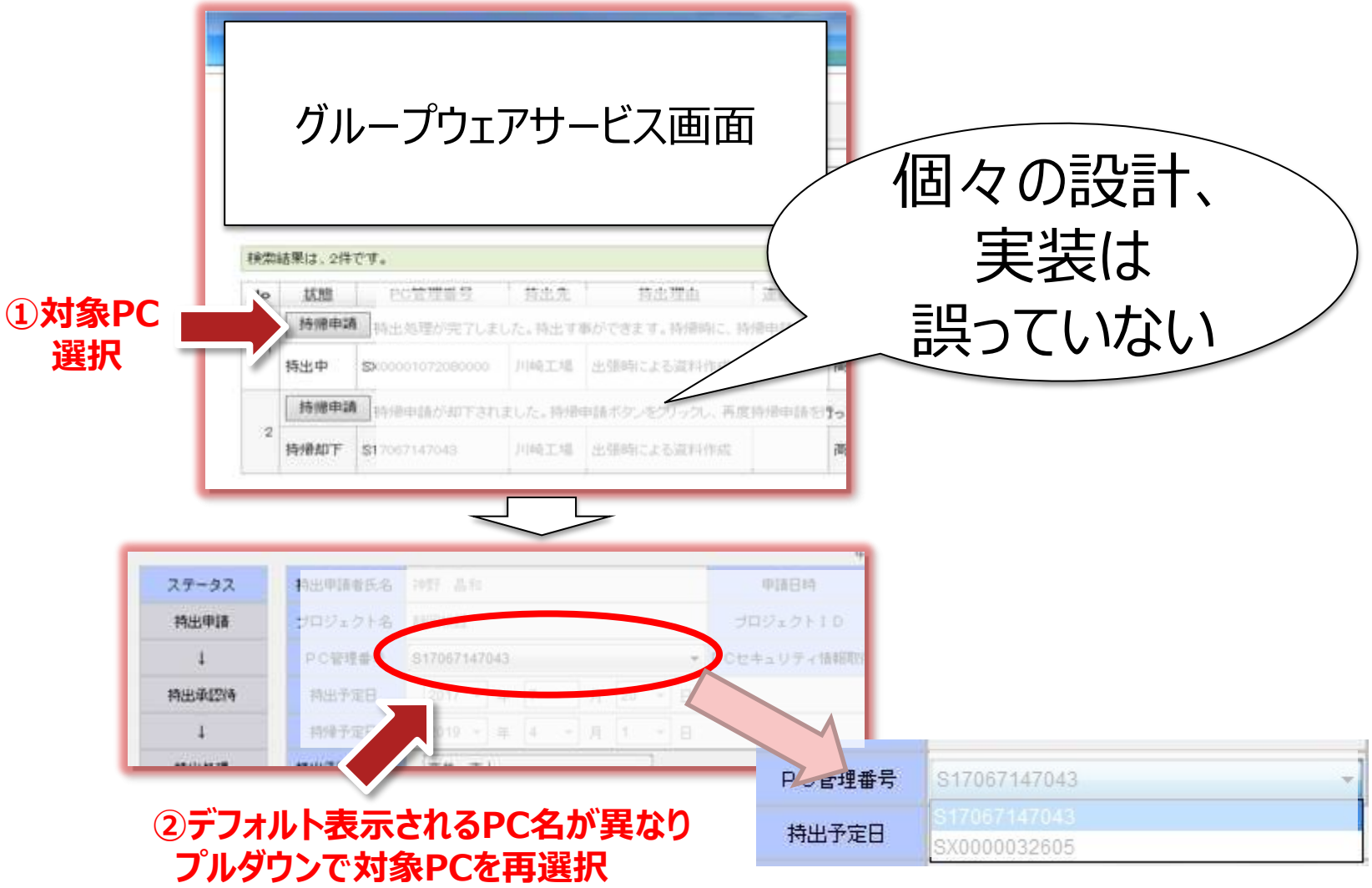
- 人と装置がやり取りする製品・サービスなどソフトウェア分野にも汎用的に使える
- 開発上流で分析ができる
- 対象システムに対する知識が深くなくても分析ができる（STAMP/STPAのスキルが高くなくても）

Copyright 2019 FUJITSU QUALITY LABORATORY LIMITED
Copyright 2019 FUJITSU COMPUTER TECHNOLOGIES LIMITED

【検証例】グループウェア・サービス

FUJITSU

■ ユーザビリティ・テストで指摘された問題

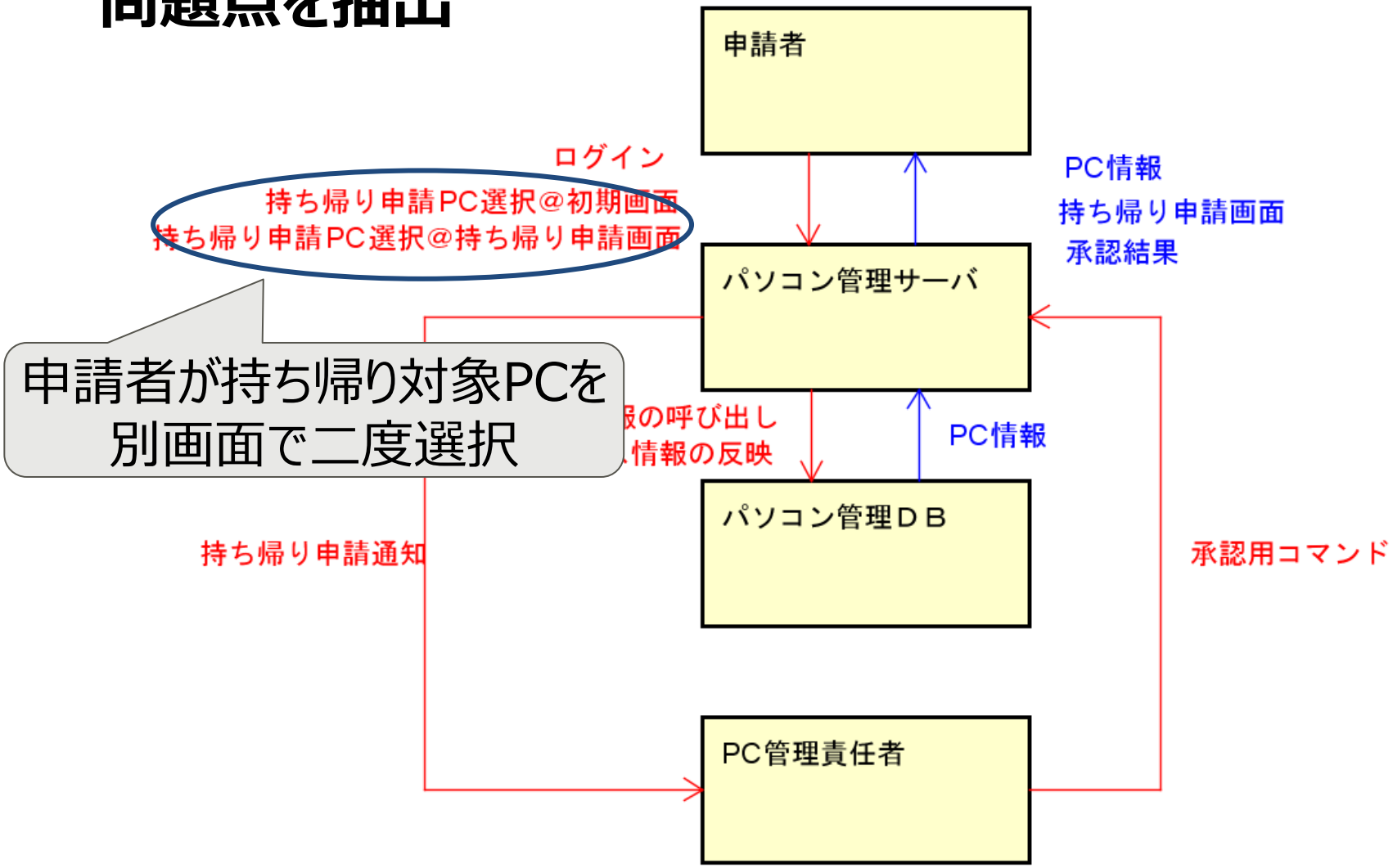


Copyright 2019 FUJITSU QUALITY LABORATORY LIMITED
Copyright 2019 FUJITSU COMPUTER TECHNOLOGIES LIMITED

【検証例】グループウェア・サービス

FUJITSU

- **開発や評価に関わっていないメンバーがSTAMPにより問題点を抽出**

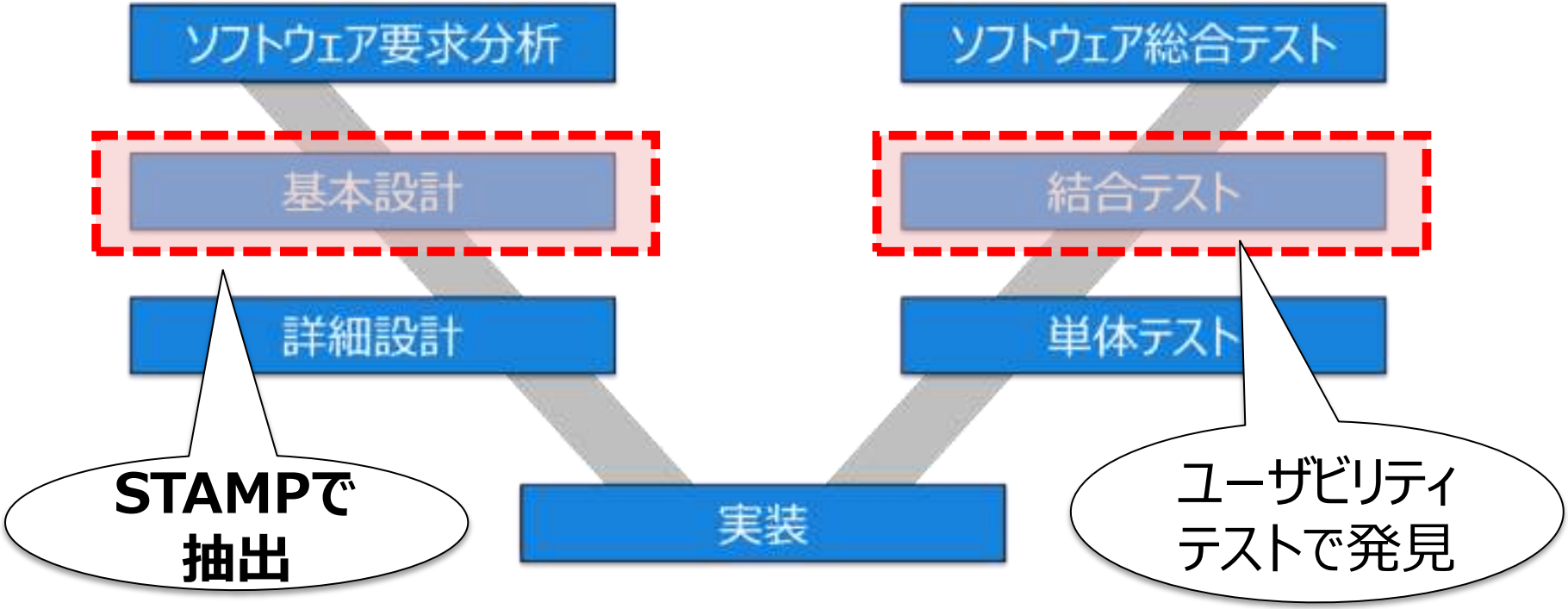


Copyright 2019 FUJITSU QUALITY LABORATORY LIMITED
Copyright 2019 FUJITSU COMPUTER TECHNOLOGIES LIMITED

【検証例】グループウェア・サービス

FUJITSU

V字開発モデルと発見工程



システムや制御の詳細を知らなくても（又は決定していなくても）、ラフな制御構造が分かれば開発上流での分析は可能！

Copyright 2019 FUJITSU QUALITY LABORATORY LIMITED
Copyright 2019 FUJITSU COMPUTER TECHNOLOGIES LIMITED

FUJITSU

1 取り巻く環境／新領域の製品・サービス開発の課題

2 失敗からの気づき／改善したいこと／本提案の着想

3 本当に STAMP/STPA は使えるのか？

4 改善のための施策

5 まとめ

6 今後の取り組み

Copyright 2019 FUJITSU QUALITY LABORATORY LIMITED
Copyright 2019 FUJITSU COMPUTER TECHNOLOGIES LIMITED

改善のための施策

FUJITSU

利用時品質を阻害する新しいタイプの損害やストレスのリスクを効果的に分析するには

発想を促す手段として、起こり得る障害やエラーをまとめ、チェックすべきポイントをモデル化（一般化、類型化）して示したもの **ヒントワード（ガイドワード）** を作成する

Copyright 2019 FUJITSU QUALITY LABORATORY LIMITED
Copyright 2019 FUJITSU COMPUTER TECHNOLOGIES LIMITED

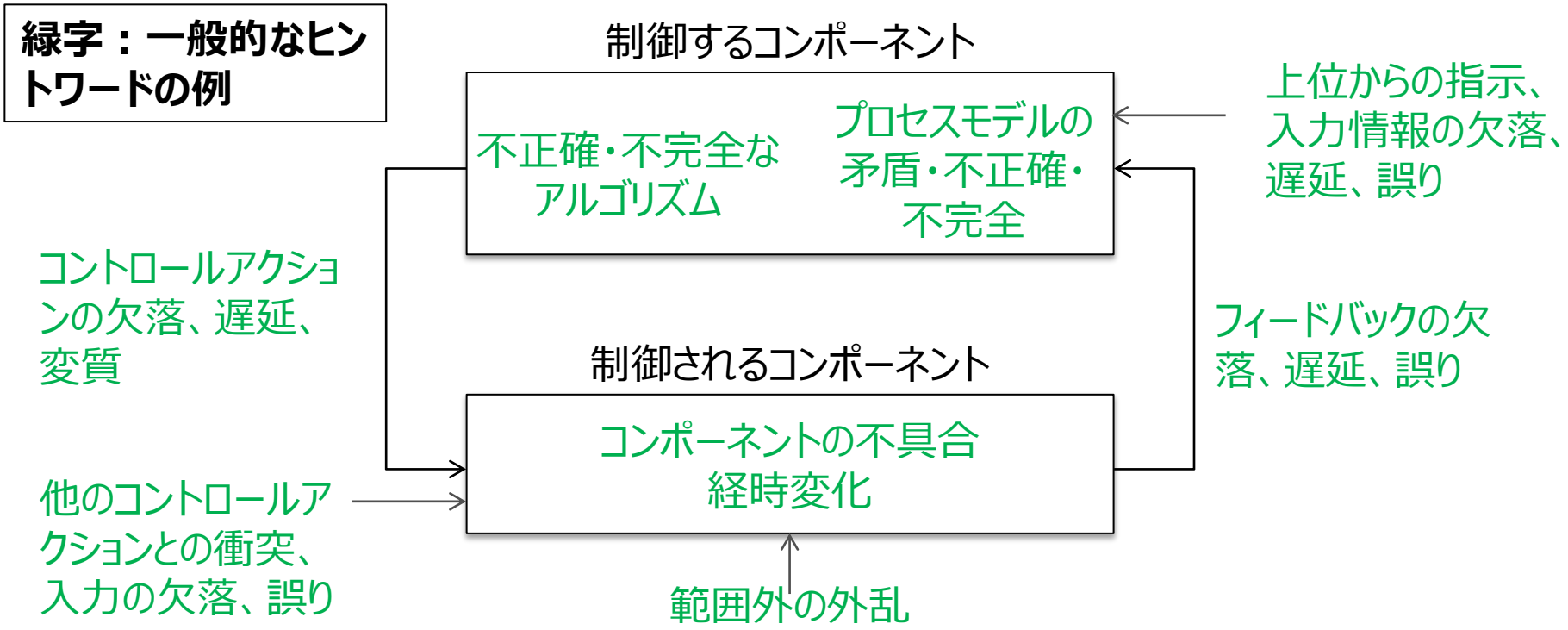
（参考）ヒントワードとは

FUJITSU

- 非安全なコントロールアクション(UCA)の一つひとつ について、それを発生させるシナリオを具体的に考える
- 考えるきっかけとして、UCAに関わるコンポーネントの周辺でチェックすべきポイントを示したもの

これによって発想が促される

緑字：一般的なヒントワードの例



Copyright 2019 FUJITSU QUALITY LABORATORY LIMITED
Copyright 2019 FUJITSU COMPUTER TECHNOLOGIES LIMITED

STAMP/STPA 適用の仮説-2

利用時品質を阻害する新しいタイプの損害やストレスのリスクに対して、ヒントワードを工夫することで効果的に分析できる

Copyright 2019 FUJITSU QUALITY LABORATORY LIMITED
Copyright 2019 FUJITSU COMPUTER TECHNOLOGIES LIMITED

施策の内容

FUJITSU

1. 利用時品質を阻害する新しいタイプの損害やストレスの事例を収集
2. 代表的な製品（例：AIスピーカー）を決め、起こり得る障害やエラーをまとめる
3. 抽出した起こり得る障害やエラーを一般化・類型化して**ヒントワード（ガイドワード）**を作る ポイント！
4. 利用時品質を阻害する新しいタイプの損害やストレスの事例でSTAMP/STPA分析を行い、作成したヒントワードの効果を検証する

Copyright 2019 FUJITSU QUALITY LABORATORY LIMITED
Copyright 2019 FUJITSU COMPUTER TECHNOLOGIES LIMITED

1. 新しいタイプの損害やストレスの事例収集

FUJITSU

事例タイトル	主要アクター			
黒人画像をゴリラと誤認識	利用者	アプリケーション	クラウドサービス	
カーナビがスラム街に「誘導」、銃撃され女性死亡　ブラジル	利用者(運転手、同乗者)	カーナビ		
テスト中のロボットが脱走、約30分暴走	テスト実施者	テスト対象ロボット	第三者	
AIスピーカー誤発注	利用者(想定外:子供)	スマートスピーカー	クラウドサービス	
	利用者(利用意図なし)	テレビ(コンテンツ含む)	スマートスピーカー	クラウドサービス
テレビCMでAIスピーカーをハック、バーガーキングの奇策	テレビ(コンテンツ含む)	スマートスピーカー	クラウドサービス	サービス利用者(第三者)
英警察が「犯罪リスク評価AI」を導入へ	利用者(警察)	被疑者	リスク評価システム	
AIスピーカーが誤作動で録音情報を本社に送信	利用者(利用意図なし)	スマートスピーカー	クラウドサービス	
スマートスピーカーが勝手にテレビを消す現象が続発	利用者(利用意図なし)	テレビ(コンテンツ含む)	スマートスピーカー	クラウドサービス
駐車場所案内	利用者	操作アプリ	クラウドサービス	
超音波によるスマートスピーカー乗っ取り	利用者(利用意図なし)	攻撃者	スマートスピーカー	クラウドサービス
AIスピーカーが突然「奇怪な声で笑いだす」問題が発生	利用者(利用意図なし)	スマートスピーカー	クラウドサービス	
オートパイロットでの事故	利用者(運転手)	自動運転システム		
コーヒー　プリペイドカード残高表示	利用者	プリペイドカード	カード読み取り・残額表示器	

Copyright 2019 FUJITSU QUALITY LABORATORY LIMITED
Copyright 2019 FUJITSU COMPUTER TECHNOLOGIES LIMITED

2. 製品で起こり得る障害やエラーをまとめる

FUJITSU

製品種類	起こり得る障害やエラー	
	機能・利用場面による分類（上位）	〃　（下位）
AIスピーカー	品物の発注	商品の間違い
		商品の属性（例：サイズ、色）の間違い
		数量の間違い
		数量単位（例：個、ダース）の間違い
		配送先の間違い
		配送オプション（例：日時、手段）の間違い
	サービスの予約・発注（例：乗車券、宿泊、飲食店・各種施設、レンタカー、映画演劇・アトラクション、見学・視察）	日時の間違い
		数（例：人数、チケット枚数）、構成（例：大人/こども、男女）の間違い
		内容の間違い
		情報欠落により不成立
		予約・発注にかかる制限項目の承認可否（例：「予約の場合は2時間まで」）、同意事項の承認可否が不明
		予約・発注できないときの代替案の承認可否が不明（例：「30分前ならば予約可能」）
		オプション等の選択が不適切
	操作指示（例：照明オン/オフ）	制御対象（例：対象の家電機器）の間違い
		制御内容（例：設定時間、設定温度、録画番組名、オプション類）の間違い
	操作予約（例：エアコン、放送の録画）	制御対象（例：対象の家電機器）の間違い
		制御内容（例：設定時間、設定温度、録画番組名、オプション類）の間違い
	伝言、連絡（送信）	相手先の間違い
		内容の間違い

Copyright 2019 FUJITSU QUALITY LABORATORY LIMITED
Copyright 2019 FUJITSU COMPUTER TECHNOLOGIES LIMITED

2. 製品で起こり得る障害やエラーをまとめる

FUJITSU

一般化・類型化したワード群

製品種類	起こり得る障害やエラー		(1) Not Providing(操作忘れ)				(2) Providing caused hazard(操作ミス)						
	機能・		(HC1-1)指示を必要と思っていない(知識不足)	(HC1-2)指示を知っていたが忘れる(多忙、訓練不足、割り込み)	(HC1-3)指示をしたつもり(訓練不足、確認手順が不適切)	(HC1-4)指示・フィードバックを見逃して操作をしない(指示・表示が不適切)	(HC2-1)指示内容を間違える(知識不足、訓練不足、マニュアル不適切)	(HC2-2)思い出す・手間取って遅れる(同上)	(HC2-3)指示内容を勘違い(取り違え)(同上)	(HC2-4)違う相手に指示を出す(同上)	(HC2-5)フィードバックを誤解して間違った操作を行う(同上)	(HC2-6)確認せずに見込みで指示を出す	(MP3-1)指示が来たが受けれない(故障)
AIスピーカー	品物の発注	商品の間違い		●	●	●	●		●				●
		商品の属性(例:サイズ、色)の間違い	●	●	●	●	●		●				●
		数量の間違い	●	●	●	●	●		●				●
		数量単位(例:個、ダース)の間違い	●	●	●	●	●		●				●
		配送先の間違い	●	●	●	●				●		●	●
		配送オプション(例:日時、手段)の間違い	●	●	●	●	●		●		●	●	●
	サービスの予約・発注(例:乗車券、宿泊、飲食店・各種施設、レンタカー、映画演劇・アトラクション、見学・視察)	日時の間違い			●	●	●		●		●	●	●
		数(例:人数、チケット枚数)、構成(例:大人/こども、男女)の間違い	●	●	●	●	●		●		●	●	●
		情報欠落により不成立	●	●	●	●	●		●	●	●	●	●
		予約・発注にかかる制限項目の承認可否(例:「予約の場合は2時間まで」)、同意事項の承認可否が不明	●	●	●	●		●	●		●		●
		予約・発注できないときの代替案の承認可否が不明(例:「30分前ならば予約可能」)、オプション等の選択が不適切	●	●	●	●	●	●	●		●		●

Copyright 2019 FUJITSU QUALITY LABORATORY LIMITED
Copyright 2019 FUJITSU COMPUTER TECHNOLOGIES LIMITED

3. エラーを類型化・一般化したヒントワード作成

FUJITSU

制御するコンポーネント（人）

(1) Not Providing（操作忘れ）

(HC1-1)指示を必要と思っていない（知識不足）
(HC1-2)指示を知っていたが忘れる（多忙、訓練不足、割り込み）
(HC1-3)指示をしたつもり（訓練不足、確認手順が不適切）
(HC1-4)指示・フィードバックを見逃して操作をしない（指示・表示が不適切）

(2) Providing caused hazard（操作ミス）

(HC2-1)指示内容を間違える（知識不足、訓練不足、マニュアル不適切）
(HC2-2)思い出す・手間取って遅れる（同上）
(HC2-3)指示内容を勘違い（取り違え）（同上）
(HC2-4)違う相手に指示を出す（同上）
(HC2-5)フィードバックを誤解して間違った操作を行う（同上）
(HC2-6)確認せずに見込みで指示を出す

(7) 他のコントローラー、環境

(E7-1)他のコントロールの入力か欠けている、間違っている
(E7-2)外部からの情報が欠けている、間違っている

(5) 指示（操作：スイッチ, タッチパネル, 音声など）

(A5-1)指示が伝わらない（故障、不適切なアルゴリズム）
(A5-2)指示が遅れる（故障、不適切なアルゴリズム）
(A5-3)間違った指示の混入

(6) フィードバック（画像、ランプ、振動、音声など）

(F6-1)フィードバックが伝わらない（悪環境で阻害、指示手段が不適切など）
(F6-2)フィードバックが遅れる（不適切なアルゴリズム）
(F6-3)間違ったフィードバック

制御されるコンポーネント（機械）

(3) オミッションエラー

(MP3-1)指示が来たが受け取れない（故障）
(MP3-2)間違った指示で対応（不適切なアルゴリズム）

(4) コミッションエラー

(MP4-1)指示通りの実行ができない又は遅れる（故障、不適切なアルゴリズム）
(MP4-2)間違った指示で対応できない

(8) 他のコントローラー、環境

(E8-1)他のコントロールの入力か欠けている、間違っている
(E8-2)他のコントロールの入力と衝突
(E8-3)外部からの情報が欠けている、間違っている
(E8-4)外部からの許容外の外乱

Copyright 2019 FUJITSU QUALITY LABORATORY LIMITED
Copyright 2019 FUJITSU COMPUTER TECHNOLOGIES LIMITED

4. 新しいタイプの損害やストレスの事例で検証

FUJITSU

■ カーナビがスラム街に「誘導」、銃撃され女性死亡　ブラジル

（例）

事例タイトル	カーナビがスラム街に「誘導」、銃撃され女性死亡　ブラジル				
発生時期	2015年10月				
発生事象	カーナビに従い観光地を目指すが、途中で危険なスラムへ誘導され妻が射殺。 カーナビアプリの道案内で車を運転してリオデジャネイロの対岸にある観光地のニテロイを目指した。ところがたどり着いたのは、治安の悪さで有名なスラム街にあるニテロイという名の路地だった。２人の車には２０発もの弾丸が撃ち込まれ、女性が死亡。				
利用者への影響	主たる機能（目的地への誘導）を満たす過程において、危険な状況になるリスク 開発メーカは、今回の事件については「残念ながら、目的地として選択されれば危険な地域への誘導も防止できない」と話している				
原因分類	☐ 正確性	☑ 完全性	☐ 一貫性	☐ 信憑性	☑ 最新性
	☐ アクセシビリティ	☐ 標準適合性	☐ 機密性	☐ 効率性	☐ 精度
	☐ 追跡可能性	☐ 理解性	☐ 可用性	☐ 移植性	☐ 回復性
影響分類	☐ 有効性	☐ 効率性	☐ 実用性	☐ 信用性	☐ 快感性
	☐ 快適性	☐ 経済リスク緩和性		☑ 健康・安全リスク緩和性	
	☐ 環境リスク緩和性		☐ 利用状況完全性		☐ 柔軟性

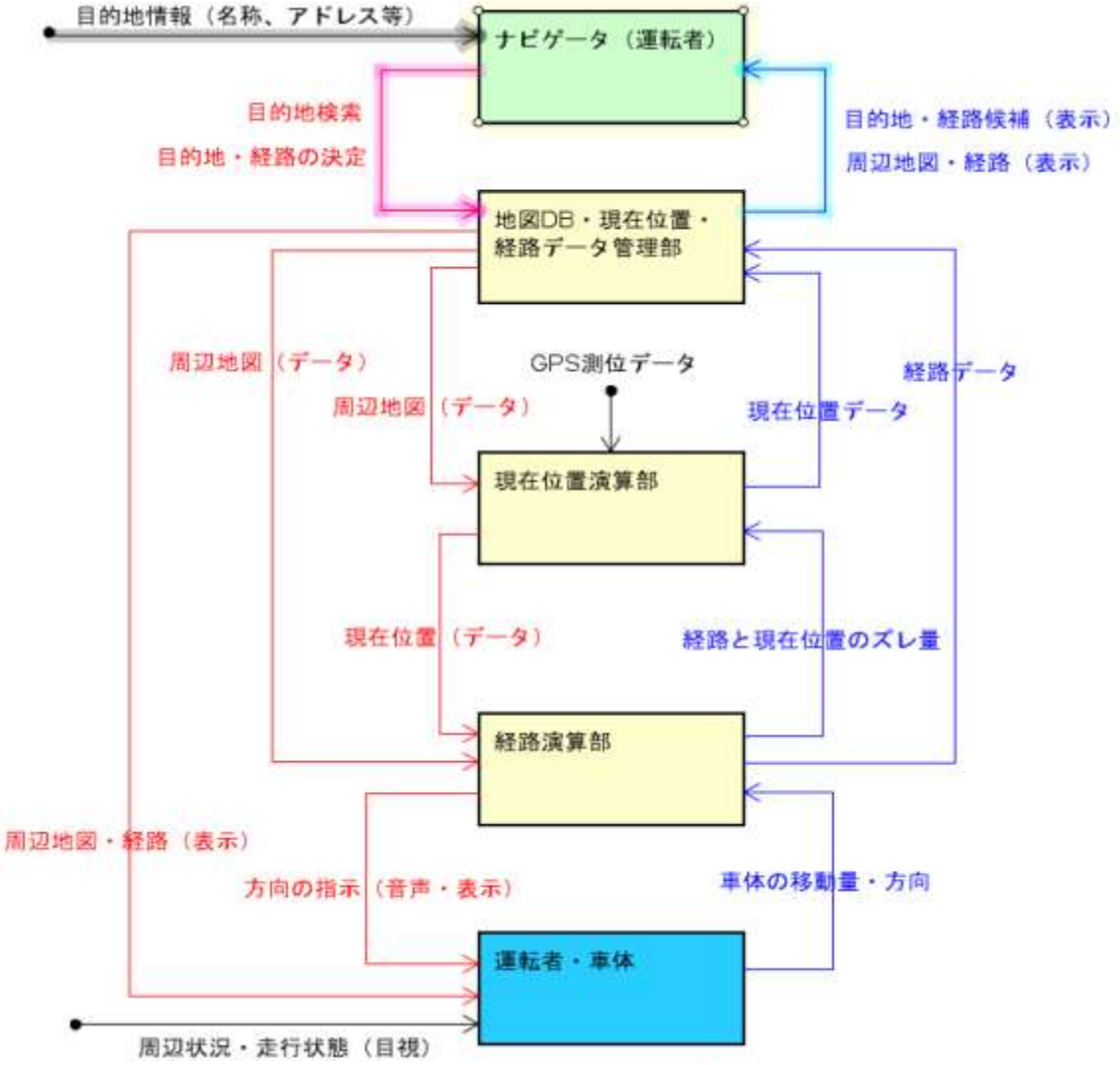
「データ品質特性:原因」と「利用時品質副特性:結果」の関係に注目して 21事例を収集

Copyright 2019 FUJITSU QUALITY LABORATORY LIMITED
Copyright 2019 FUJITSU COMPUTER TECHNOLOGIES LIMITED

【検証例】 カーナビによるアクシデント

FUJITSU

■ カーナビの制御構造図



Copyright 2019 FUJITSU QUALITY LABORATORY LIMITED
Copyright 2019 FUJITSU COMPUTER TECHNOLOGIES LIMITED

【検証例】 カーナビによるアクシデント

FUJITSU

■ 作成したヒントワードからシナリオを発想

制御するコンポーネント（人）

(1) Not Providing（操作忘れ）
(HC1-1)指示を必要と思っていない（知識不足）
(HC1-2)指示を知っていたが忘れる（多忙、訓練不足、割り込み）
(HC1-3)指示をしたつもり（訓練不足、確認手順が不適切）
(HC1-4)指示・フィードバックを見逃して操作をしない（指示・表示が不適切）

(2) Providing caused hazard（操作ミス）
(HC2-1)指示内容を間違える（知識不足、訓練不足、マニュアル不適切）
(HC2-2)思い出す・手間取って遅れる（同上）
(HC2-3)指示内容を勘違い（取り違え）（同上）
(HC2-4)違う相手に指示を出す（同上）
(HC2-5)違う相手に指示を出す（同上）
(HC2-6)フィードバックを誤解して間違った操作を行う（同上）
(HC2-7)確認せずに見込みで指示を出す

(7) 他のコントローラー、環境
(E7-1)他のコントロールの入力か欠けている、間違っている
(E7-2)外部からの情報が欠けている、間違っている

(5) 指示（操作：スイッチ, タッチパネル, 音声など）
(A5-1)指示が伝わらない（故障、不適切なアルゴリズム）
(A5-2)指示が遅れる（故障、不適切なアルゴリズム）
(A5-3)間違った指示の混入

(6) フィードバック（画像、ランプ、振動、音声など）
(F6-1)フィードバックが伝わらない（悪環境で阻害、指示手段が不適切など）
(F6-2)フィードバックが遅れる（不適切なアルゴリズム）
(F6-3)間違ったフィードバック

制御されるコンポーネント（機械）

(3) オミッションエラー
(MP3-1)指示が来たが受け取れない（故障）
(MP3-2)間違った指示で対応（不適切なアルゴリズム）

(4) コミッションエラー
(MP4-1)指示通りの実行ができない又は遅れる（故障、不適切なアルゴリズム）
(MP4-2)間違った指示で対応で

(8) 他のコントローラー、環境
(E8-1)他のコントロールの入力か欠けている、間違っている
(E8-2)他のコントロールの入力と衝突
(E8-3)外部からの情報が欠けている、間違っている
(E8-4)外部からの許容外の外乱

ID	HCF	ヒントワード	シナリオ
HCF1-P-1-1	誤った目的地を決定する（ヒューマンエラー）	(HC2-1)指示内容を間違える（知識不足）	目指す目的地に関する知識不足のため、誤った目的地を選択し決定した
HCF2-N-1-1	運転者への経路上の安全情報が欠落	(E7-2)外部からの情報が欠けている	経路上に存在する危険な場所（工事中、通行止め、事故、落下物、治安）などの安全情報が欠けており、運転者の危険に対する認知が遅れる

Copyright 2019 FUJITSU QUALITY LABORATORY LIMITED
Copyright 2019 FUJITSU COMPUTER TECHNOLOGIES LIMITED

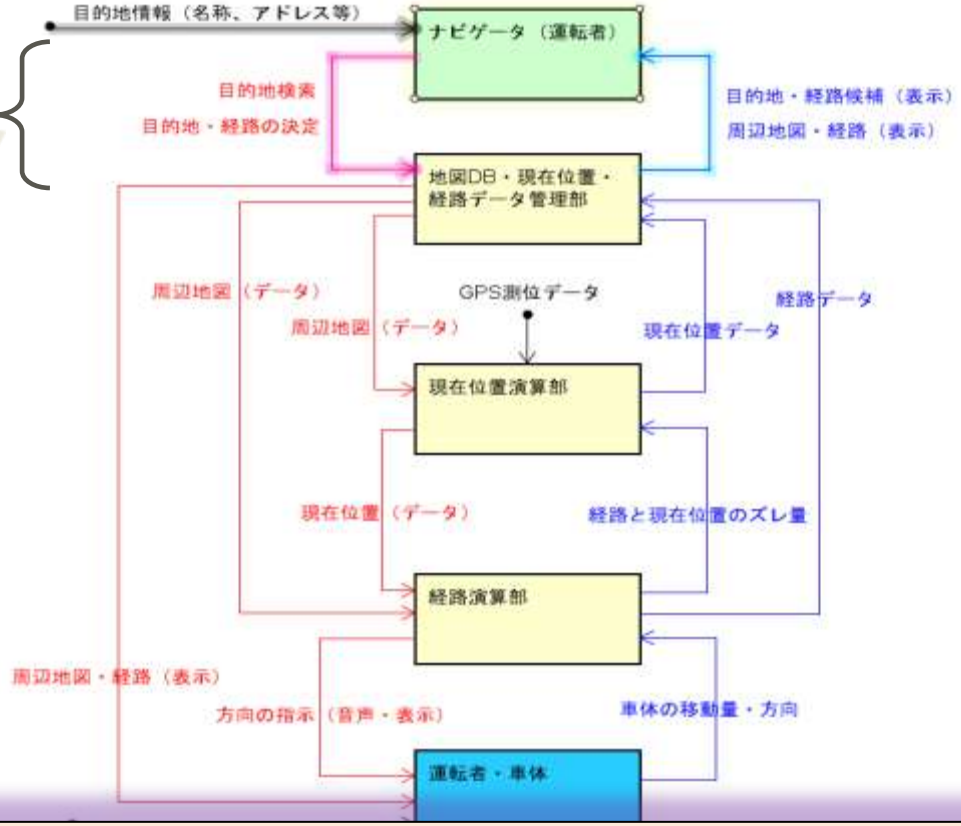
【検証例】 カーナビによるアクシデント

FUJITSU

■ カーナビの制御構造の弱点抽出

決定した目的地が、
目指す目的地かどうか
チェックできない

運転者への経路上の
安全情報が欠けている



利用時品質を阻害する新しいタイプの損害やストレスのリスクに対して、ヒントワードを工夫することで効果的に分析できる可能性あり！

Copyright 2019 FUJITSU QUALITY LABORATORY LIMITED
Copyright 2019 FUJITSU COMPUTER TECHNOLOGIES LIMITED

FUJITSU

1 取り巻く環境／新領域の製品・サービス開発の課題

2 失敗からの気づき／改善したいこと／本提案の着想

3 本当に STAMP/STPA は使えるのか？

4 改善のための施策

5 まとめ

6 今後の取り組み

Copyright 2019 FUJITSU QUALITY LABORATORY LIMITED
Copyright 2019 FUJITSU COMPUTER TECHNOLOGIES LIMITED

まとめ

FUJITSU

- 人と装置がやり取りする製品・サービスなどソフトウェア分野にも汎用的に使える
- 開発上流で分析ができる
- 対象システムに対する知識が深くなくても分析ができる（STAMP/STPAのスキルが高くなくても）

システムや制御の詳細を知らなくても（又は決定していなくても）、ラフな制御構造が分かれば開発上流での分析は可能！

利用時品質を阻害する新しいタイプの損害やストレスのリスクに対して、ヒントワードを工夫することで効果的に分析できる可能性あり！

STAMP/STPAを使ったリスク分析を開発上流に適用し、新しいタイプの損害やストレスをリスクとして事前に抽出できる可能性を検証できた

Copyright 2019 FUJITSU QUALITY LABORATORY LIMITED
Copyright 2019 FUJITSU COMPUTER TECHNOLOGIES LIMITED

FUJITSU

1 取り巻く環境／新領域の製品・サービス開発の課題

2 失敗からの気づき／改善したいこと／本提案の着想

3 本当に STAMP/STPA は使えるのか？

4 改善のための施策

5 まとめ

6 今後の取り組み

Copyright 2019 FUJITSU QUALITY LABORATORY LIMITED
Copyright 2019 FUJITSU COMPUTER TECHNOLOGIES LIMITED

今後の取り組み

FUJITSU

- STAMP/STPAを使った事例を増やし、社内教育やワークショップなどの開催で組織としての底上げを図る
- 対象（製品、機能）の範囲を広げてヒントワード（ガイドワード）集のバリエーションを増やす
- 作成したヒントワード集は社内のリポジトリなどに登録し、「プロセス資産」として利活用しやすくする
- STAMP/STPA分析手法は、当社の標準プロセスとして規定・ガイドライン化する

Copyright 2019 FUJITSU QUALITY LABORATORY LIMITED
Copyright 2019 FUJITSU COMPUTER TECHNOLOGIES LIMITED

ご静聴ありがとうございました

Copyright 2019 FUJITSU QUALITY LABORATORY LIMITED
Copyright 2019 FUJITSU COMPUTER TECHNOLOGIES LIMITED

FUJITSU

shaping tomorrow with you