SPI Japan 2020 発表資料

FUJITSU
shaping tomorrow with you

開発SEが使える！　今注目のリスク分析手法 STAMP/STPAのシステム開発への適用

システム開発でのSTAMP/STPAの実践を通じて得られたテーラリングのエッセンス

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

目次

FUJITSU

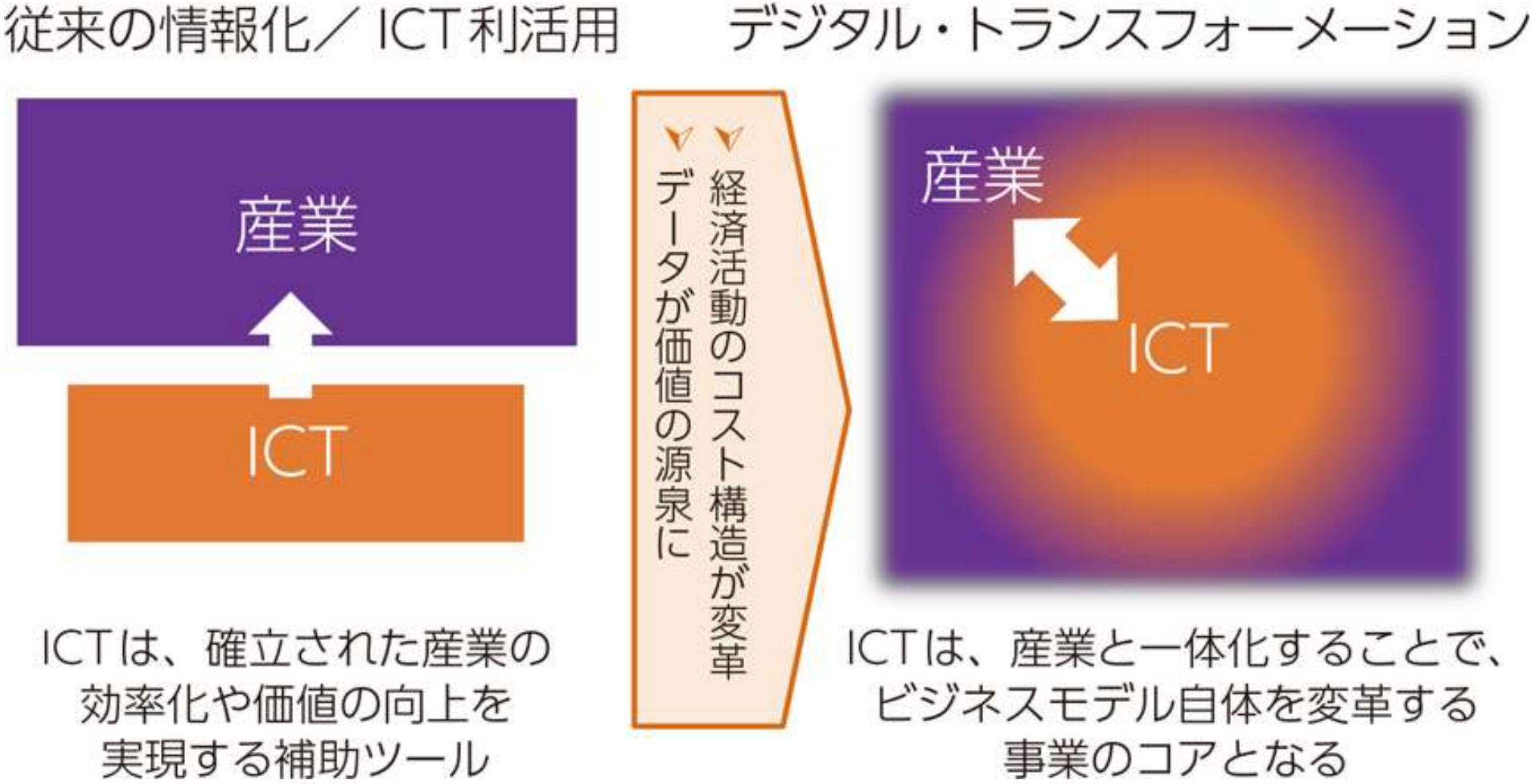
開発SEが使える！　今注目のリスク分析手法STAMP/STPAのシステム開発への適用

～　システム開発でのSTAMP/STPAの実践を通じて得られたテーラリングのエッセンス　～

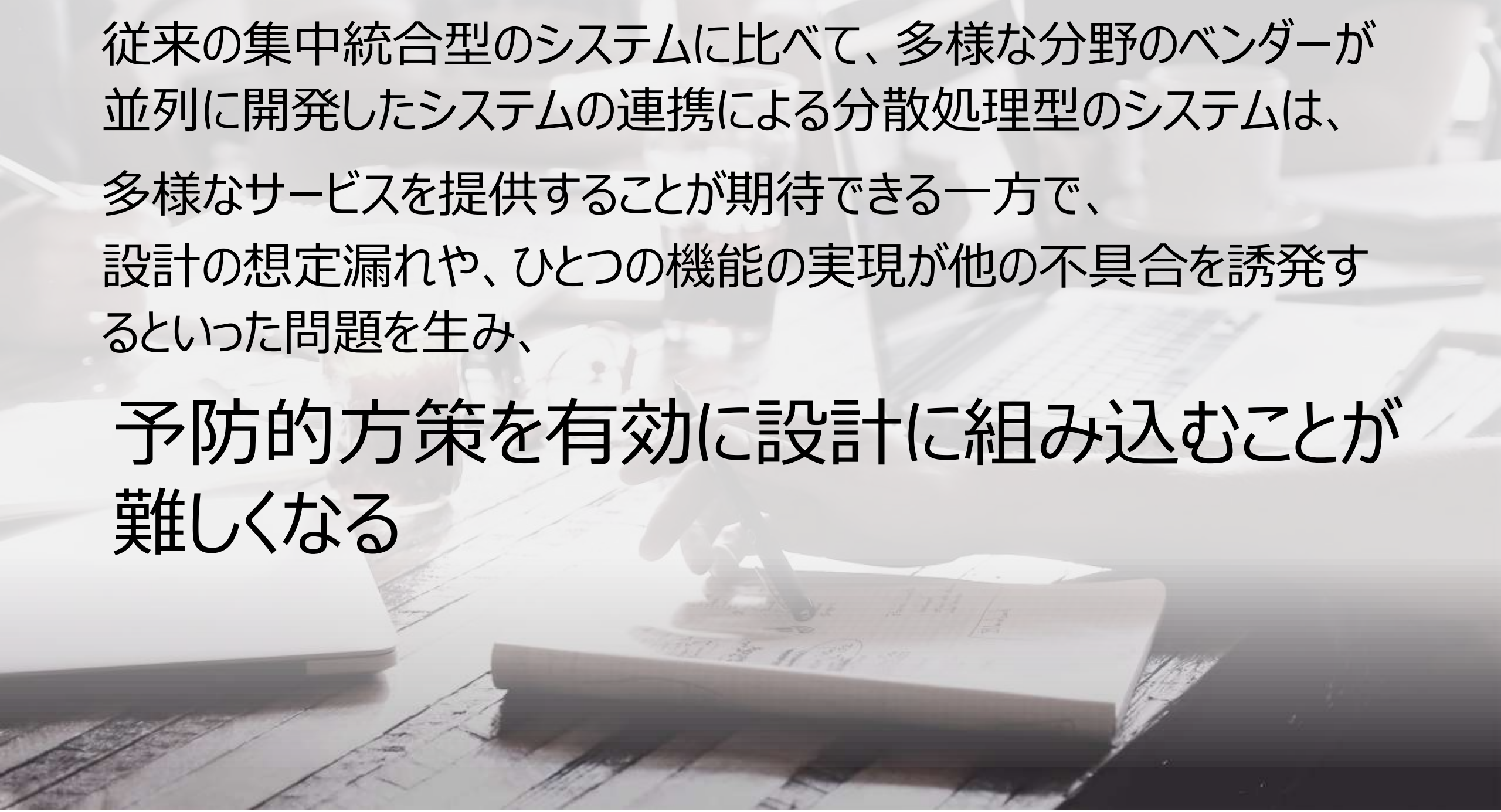
- 何が課題か
- 何を改善したいか
- STAMP/STPA とは
- どのような方法をとったのか
- 効果は何か　どのような成果が得られたか
- 残存課題

- 何が課題か
- 何を改善したいか
- STAMP/STPA とは
- どのような方法をとったのか
- 効果は何か　どのような成果が得られたか
- 残存課題

データが価値の源泉となる新しいビジネス領域のシステムは、外部システムと複雑につながり、よりダイナミックに変化



変化に対応するためのデジタル・トランスフォーメーション　総務省，令和元年版　情報通信白書



従来の集中統合型のシステムに比べて、多様な分野のベンダーが並列に開発したシステムの連携による分散処理型のシステムは、

多様なサービスを提供することが期待できる一方で、
設計の想定漏れや、ひとつの機能の実現が他の不具合を誘発するといった問題を生み、

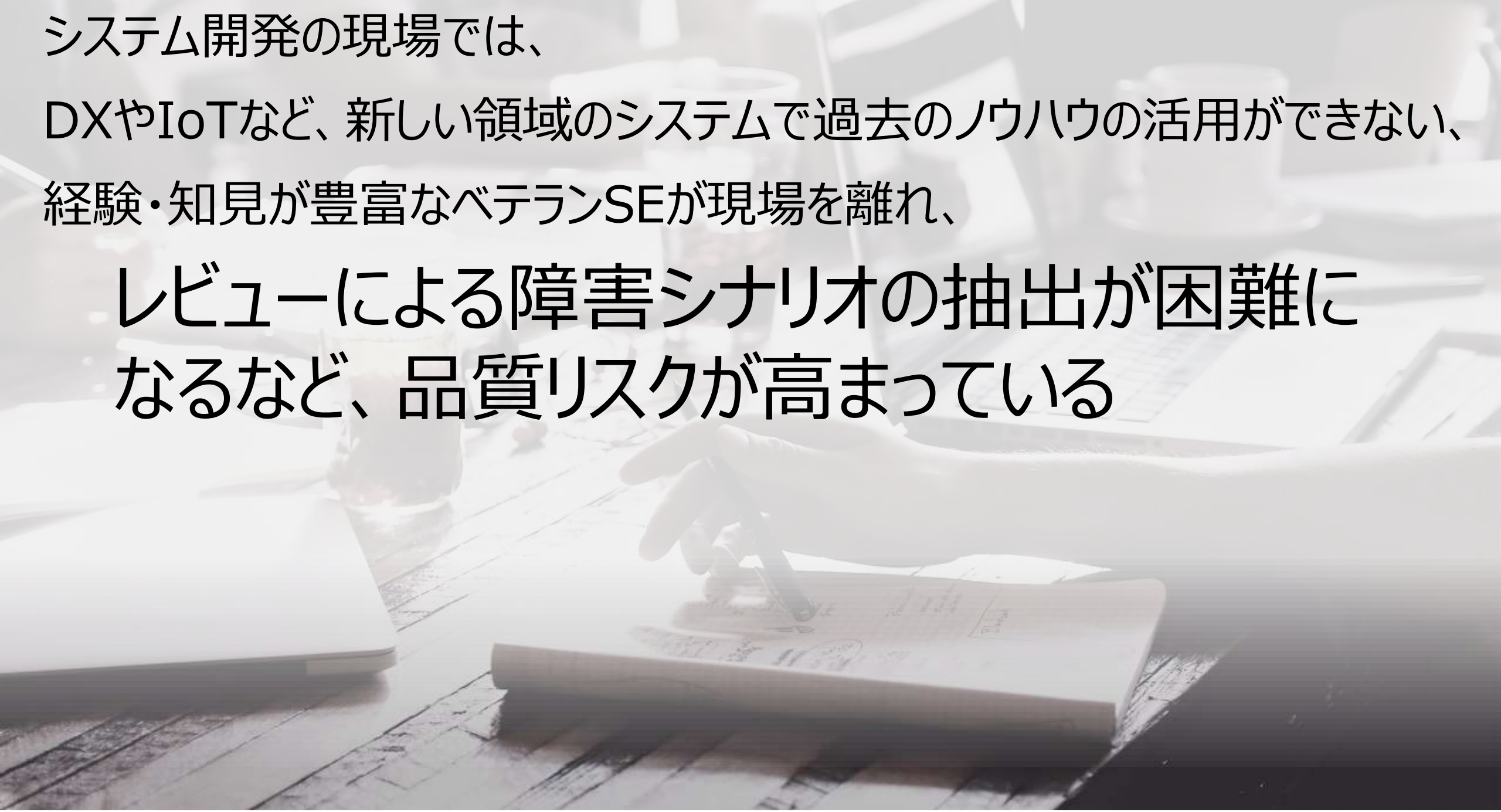
予防的方策を有効に設計に組み込むことが難しくなる

システム開発の現場では、

DXやIoTなど、新しい領域のシステムで過去のノウハウの活用ができない、

経験・知見が豊富なベテランSEが現場を離れ、

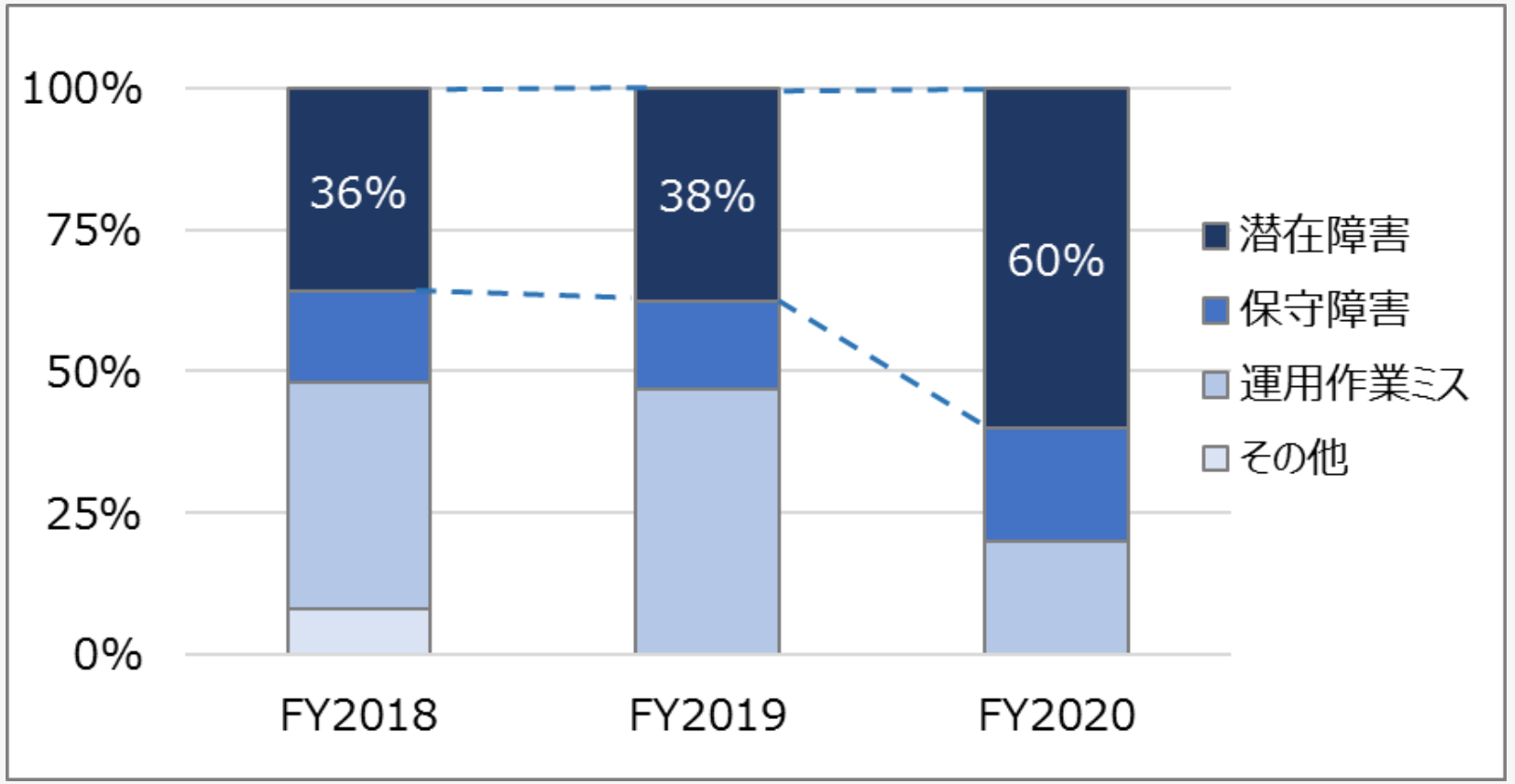
レビューによる障害シナリオの抽出が困難になるなど、品質リスクが高まっている



その結果、

開発で作り込んだ潜在障害が年々増加傾向にある

SE起因のシステムトラブル状況（原因別）



※当社収集データより

こうした課題認識を背景に

システム開発にSTAMP/STPAを取り入れ
新しいリスク分析手法として活用しようとする潮流が、
システム開発の現場にも起こり始めている

しかし・・・

分析の手順を一通り学習したにも関わらず、

技術者が容易に分析を実施できる状況ではなかった

FUJITSU

開発SEが使える！　今注目のリスク分析手法STAMP/STPAのシステム開発への適用

～　システム開発でのSTAMP/STPAの実践を通じて得られたテーラリングのエッセンス　～

- 何が課題か
- 何を改善したいか
- STAMP/STPA とは
- どのような方法をとったのか
- 効果は何か　どのような成果が得られたか
- 残存課題

FUJITSU

当社主催のSTAMP/STPAセミナーやワークショップに参加した技術者の声

- 「用語が難しい」
- 「導入書を読んでも分からない」
- 「どこまで分析をしたらよいか分からない」

もともと　STAMP/STPAは、
主に動的システムの安全性解析手法として、安全性を重視する
航空宇宙や自動車分野を中心に導入が進んできたため、

静的システムの開発におけるリスク分析に適した
道具立てやプロセスのテーラリングが出来ていない
ことが原因 と考察

何を改善したいか

STAMP/STPAの知見・経験が少ない技術者（開発SEを想定）が、

1. 自律的な分析を実施できる

2. 障害シナリオを効果的に抽出できる

3. 重要障害の未然防止につながる対策を設計に織り込むことができる

FUJITSU

開発SEが使える！　今注目のリスク分析手法STAMP/STPAのシステム開発への適用

～　システム開発でのSTAMP/STPAの実践を通じて得られたテーラリングのエッセンス　～

- 何が課題か
- 何を改善したいか
- STAMP/STPA とは
- どのような方法をとったのか
- 効果は何か　どのような成果が得られたか
- 残存課題

STAMPの概念

「STAMP：システム理論に基づくアクシデントモデル」

STAMP（**S**ystem-**T**heoretic **A**ccident **M**odel and **P**rocesses）

前提

事故の多くは、構成要素の故障ではなく、システムの中での安全のための
制御を行う コンポーネント間（制御要素と非制御要素）の
相互作用が働かない事によって起こる

FUJITSU

「相互作用」が働かないって
どういうことでしょう？

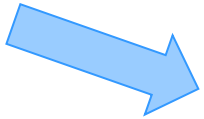
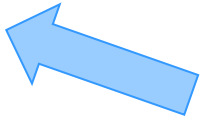
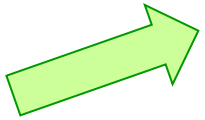
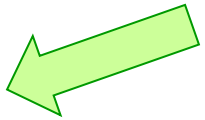
ユーバーリンゲン
空中衝突事故
(2002年 ドイツ)

（画像：Unsplash）

「相互作用が働かない」

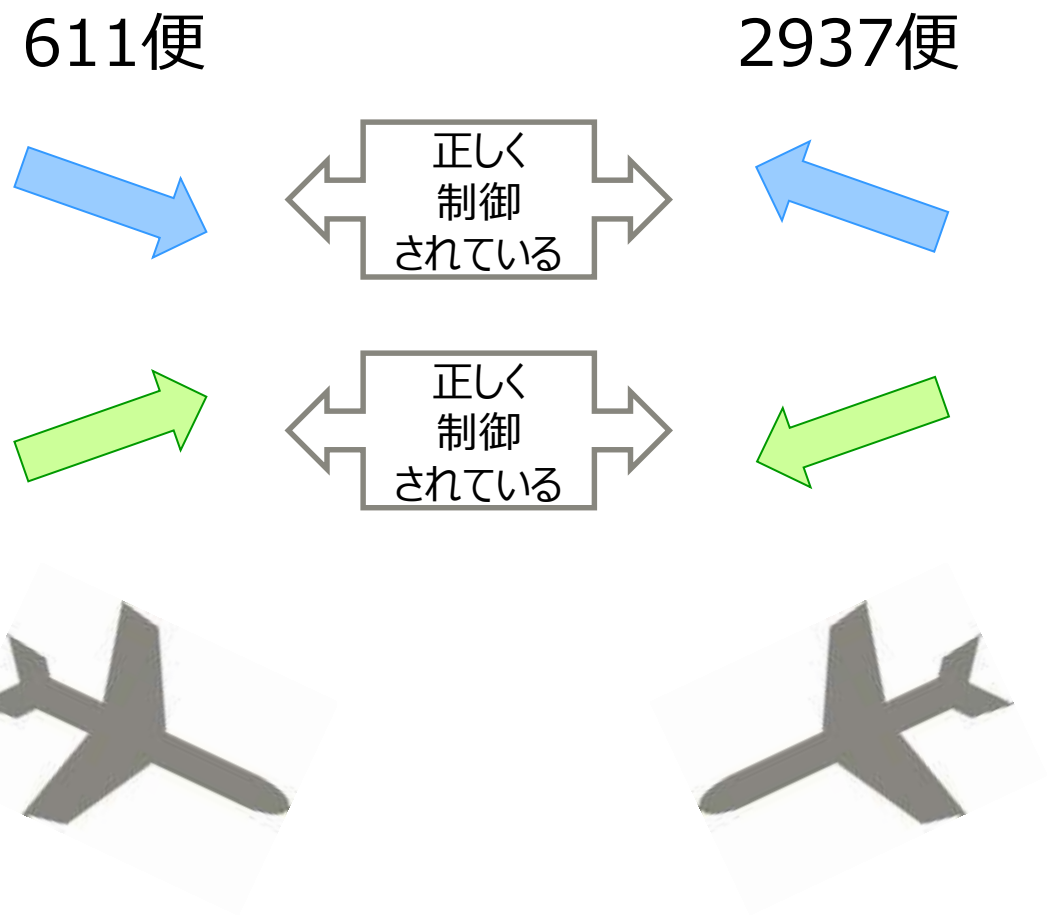
FUJITSU

ユーバーリンゲン空中衝突事故(2002年 ドイツ)

	611便	2937便
TCAS（空中衝突防止装置）の指示		
地上管制官の指示		
パイロットの操作		

「相互作用が働かない」

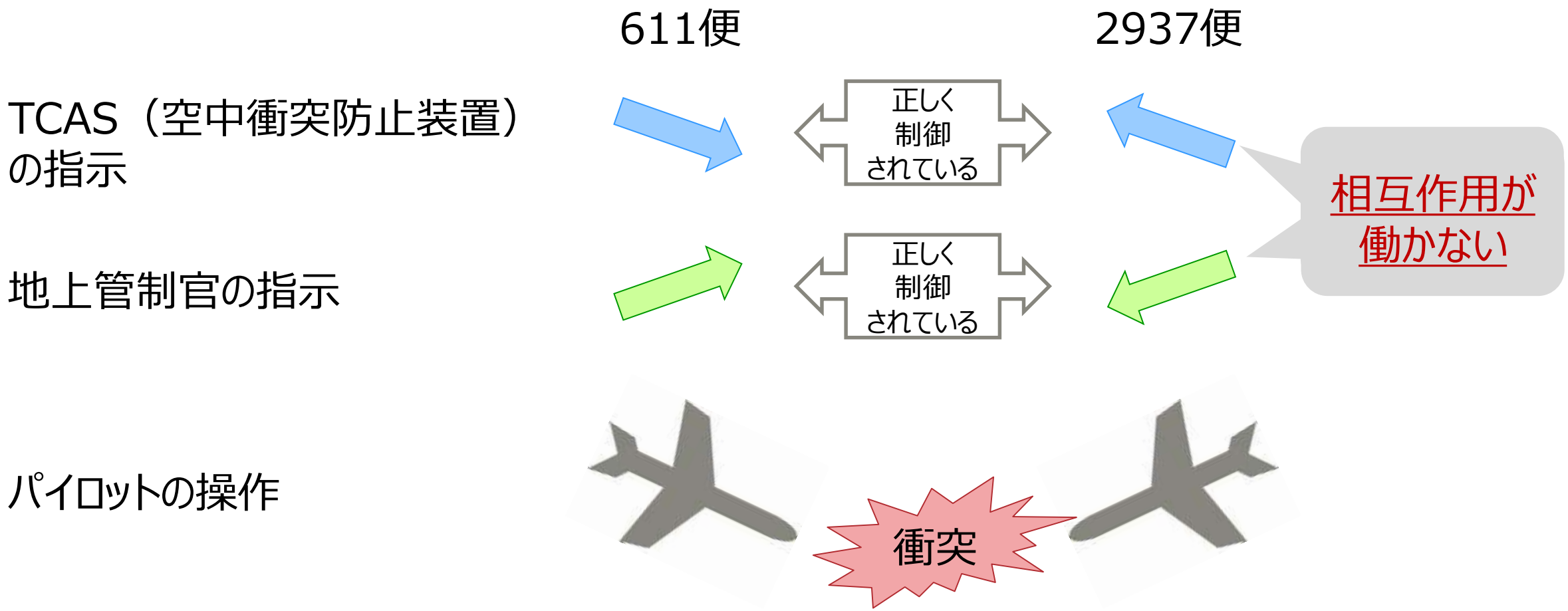
ユーバーリンゲン空中衝突事故(2002年 ドイツ)



「相互作用が働かない」

FUJITSU

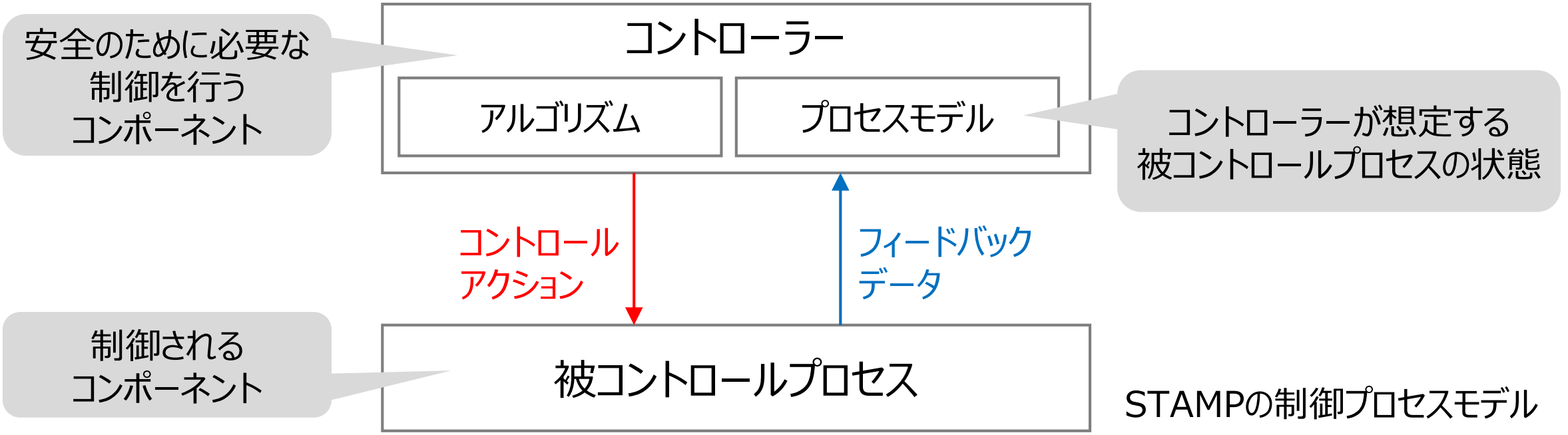
ユーバーリンゲン空中衝突事故(2002年 ドイツ)



STAMPの概念

- 「要素（コンポーネント）」と「相互作用（コントロールアクション）」に着目してメカニズムを説明

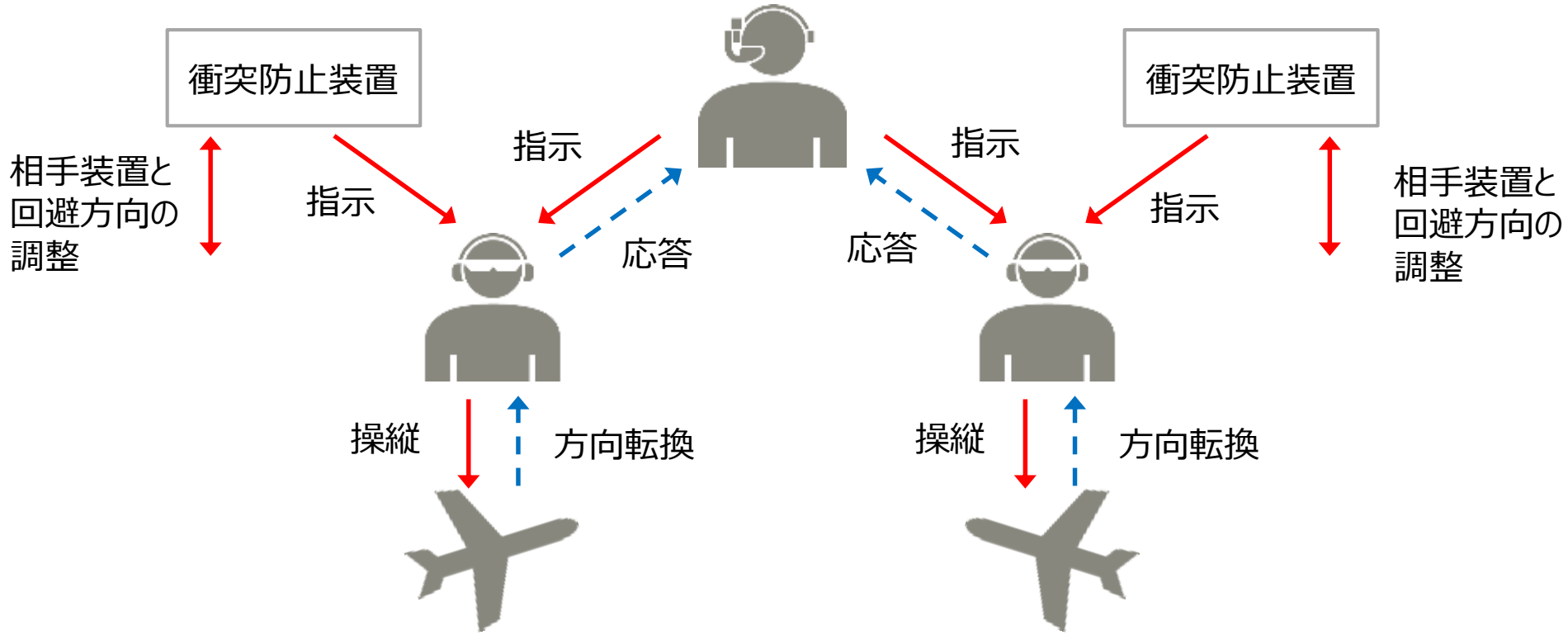
- 「相互作用が働かない原因」＝「コントロールアクションの不適切な作用」という視点を持つことで原因を有限化



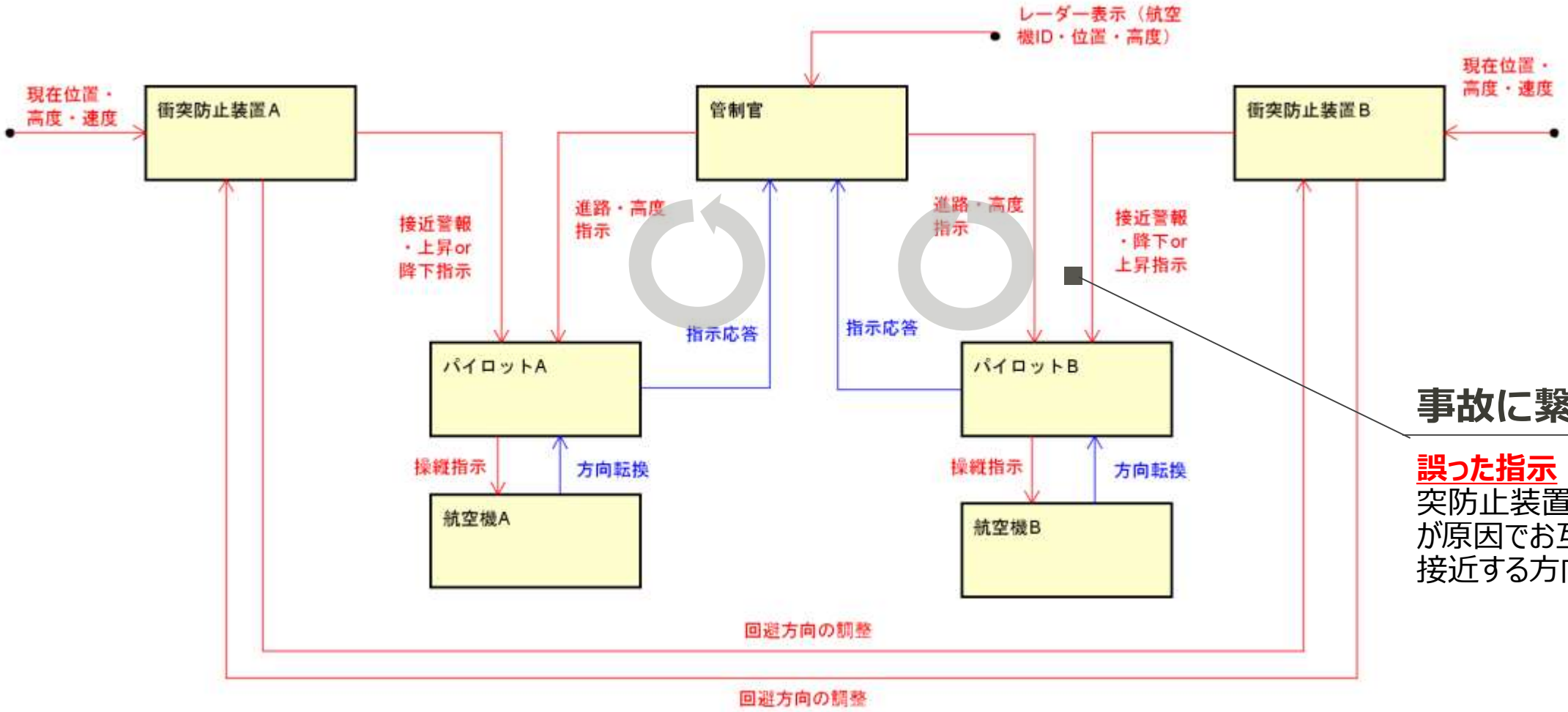
STAMPの制御プロセスモデル

「要素」と「相互作用」に着目する

例）ユーバーリンゲン事故の「要素（コンポーネント)」と「相互作用(コントロールアクション)」のモデル



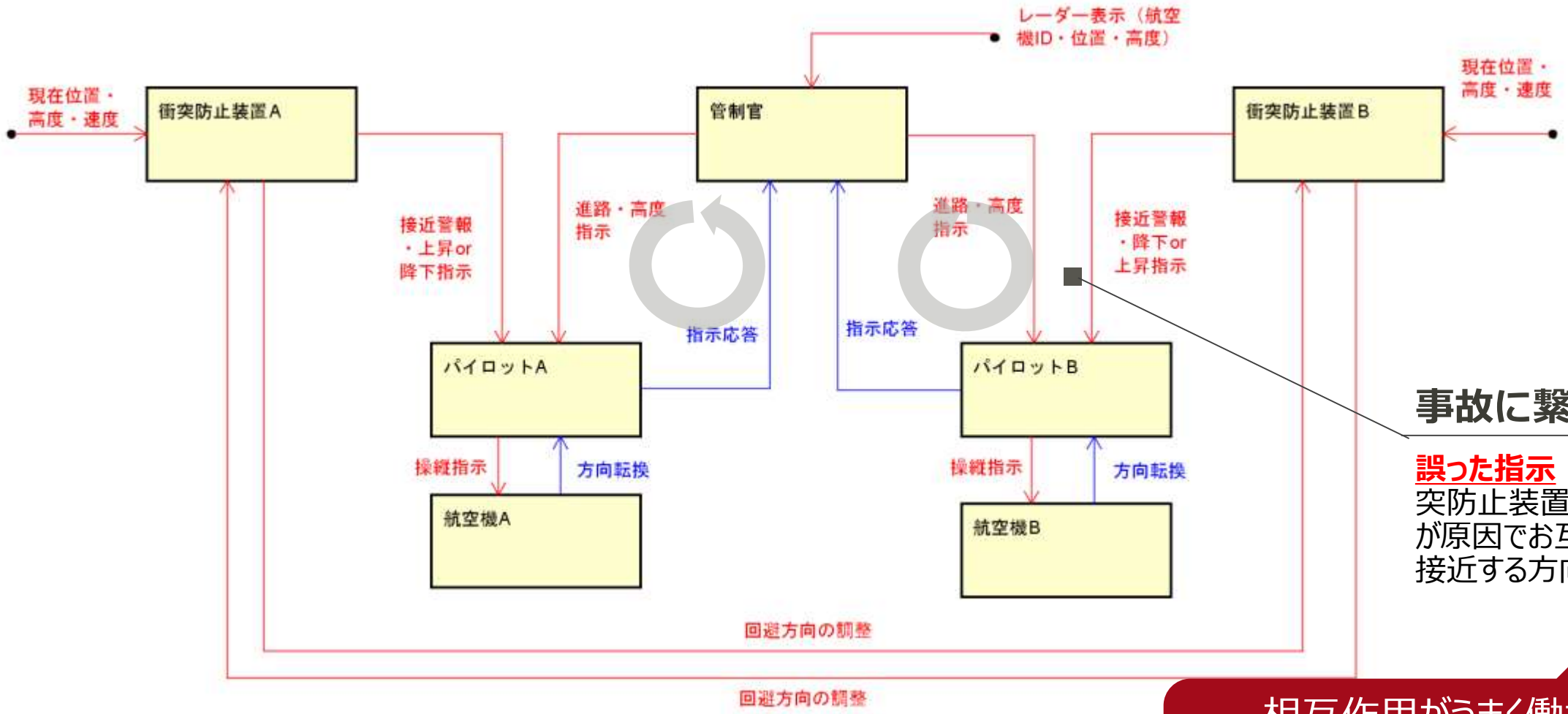
STAMPのキモ：制御構造図



事故に繋がるシナリオ

誤った指示：管制官から指示が衝突防止装置の指示と異なり、それが原因でお互いのパイロットがより接近する方向に操縦桿をきる

STAMPのキモ：制御構造図



事故に繋がるシナリオ

誤った指示：管制官から指示が衝突防止装置の指示と異なり、それが原因でお互いのパイロットがより接近する方向に操縦桿をきる

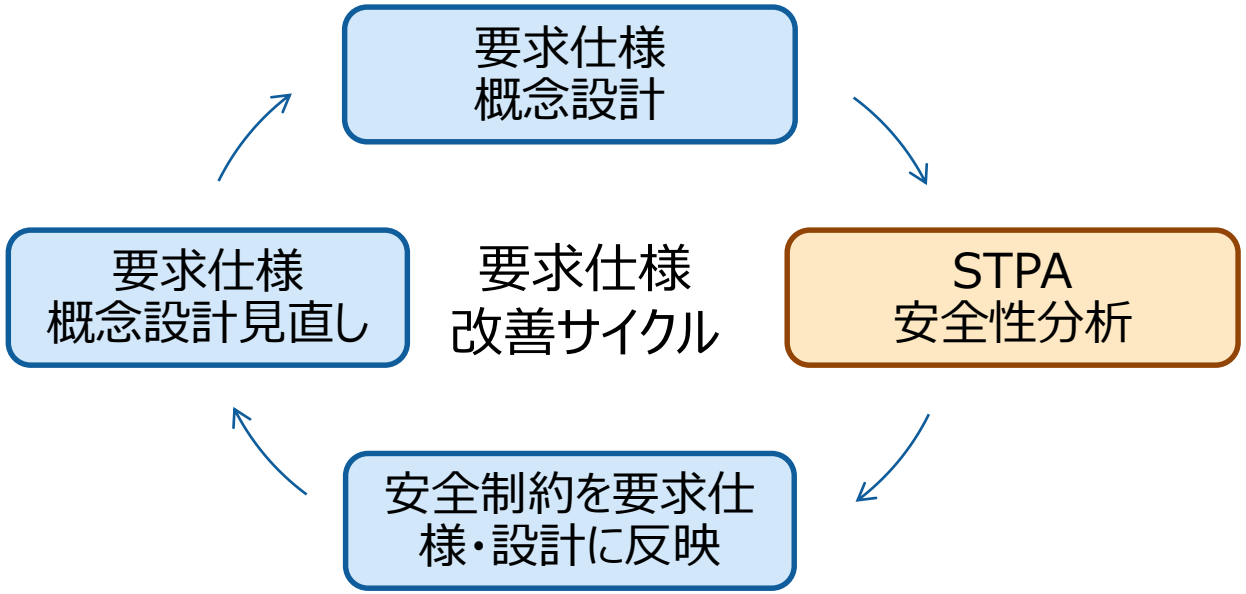
相互作用がうまく働かない原因
異なった指示が来た場合の
ルールが決まっていない

STPAとは？

「STPA：STAMPアクシデントモデルに基づく安全解析手法」

STPA（**S**ystems-**T**heoretic **P**rocess **A**nalysis ）

- 全体俯瞰の上で、トップダウンで分析を実施
- 手段（How）ではなく、Whatに着目した手法
- 概念設計の段階で、安全性を高めるための要求仕様・概念設計の見直し(フィードバック)ができる



従来の分析手法

FTA（ Fault Tree Analysis：故障・事故の分析手法）の例

従来の分析手法

FUJITSU

FTA（ Fault Tree Analysis：故障・事故の分析手法）の例

機器やコンポーネントの単一故障やソフトウェアバグを
要因として識別

従来の分析手法

FTA（ Fault Tree Analysis：故障・事故の分析手法）の例

分岐条件を論理的に組む（How）ことで深く、網羅的に分析できる反面全体的な視野での分析が難しい

機器やコンポーネントの単一故障やソフトウェアバグを要因として識別

STPAによる分析手順-1

Step 0（準備1）
損失(アクシデント), 危険な状態(Hazard), 安全制約の識別

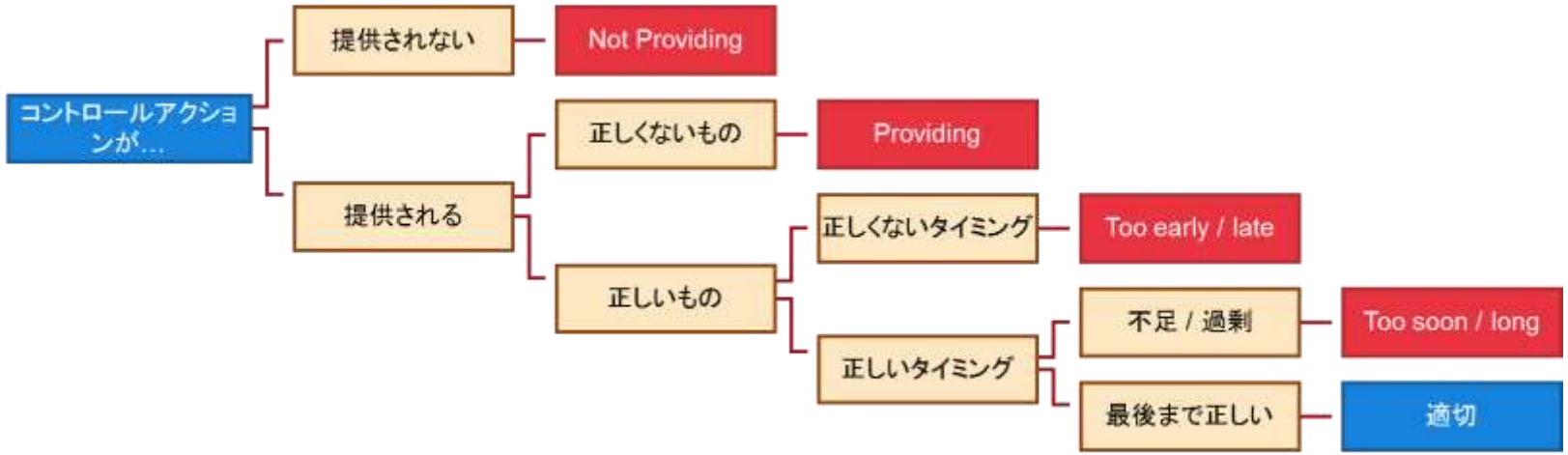
Step 0（準備2）
制御構造図の構築

Step 1
非安全な制御・指示による危険な状態につながるシナリオ分析

Step 2
危険な状態につながる要因の識別

対策検討

Step1.
４つのガイドワードを用いて、危険な状態を導くコントローラーの動作を網羅的に識別



STPAによる分析手順-2

Step 0（準備1）
損失(アクシデント), 危険な状態(Hazard), 安全制約の識別

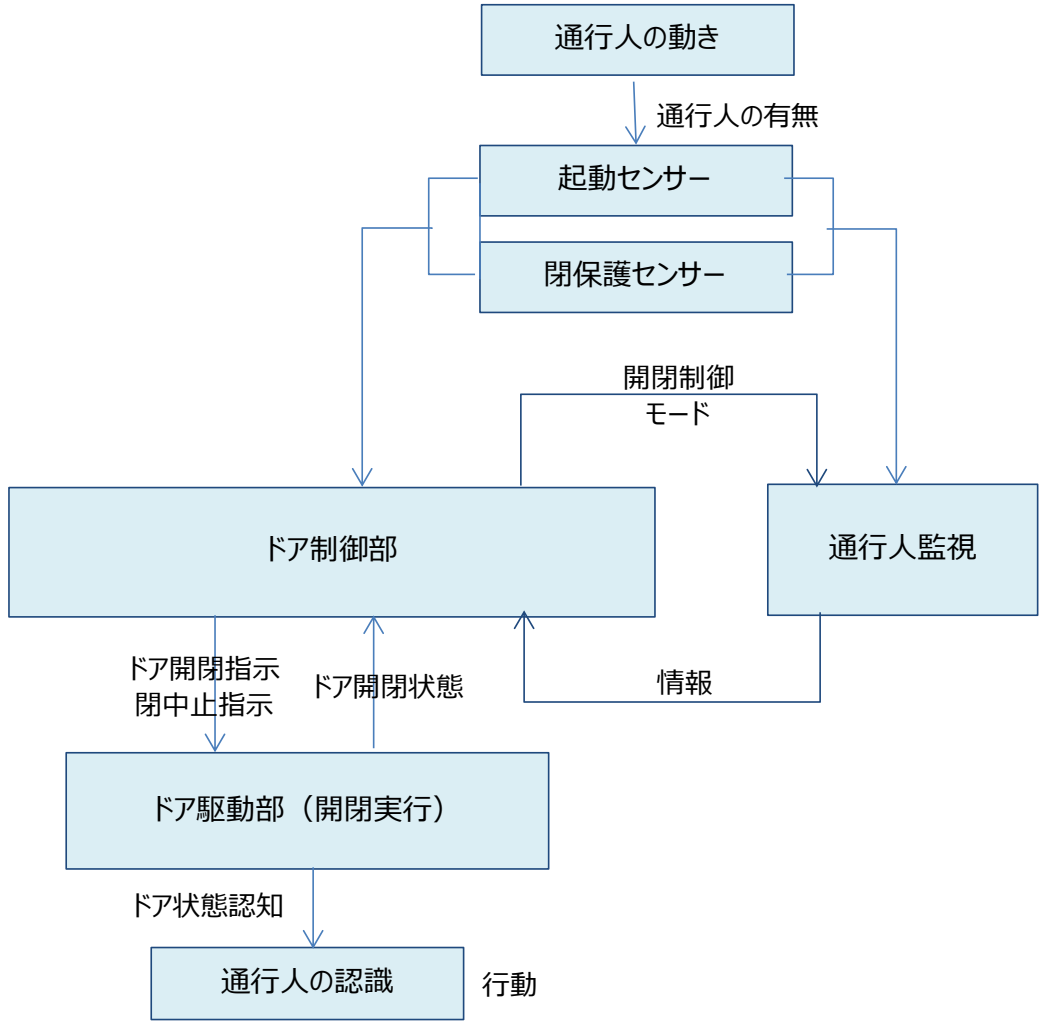
Step 0（準備2）
制御構造図の構築

Step 1
非安全な制御・指示による危険な状態につながるシナリオ分析

Step 2
危険な状態につながる要因の識別

対策検討

Step2.
ソフトウェア、人間、外部システム、環境に起因する要因として、あるべき状態と矛盾することで起きる要因を識別する



STPAによる分析手順-2

Step 0（準備1）
損失(アクシデント), 危険な状態(Hazard), 安全制約の識別

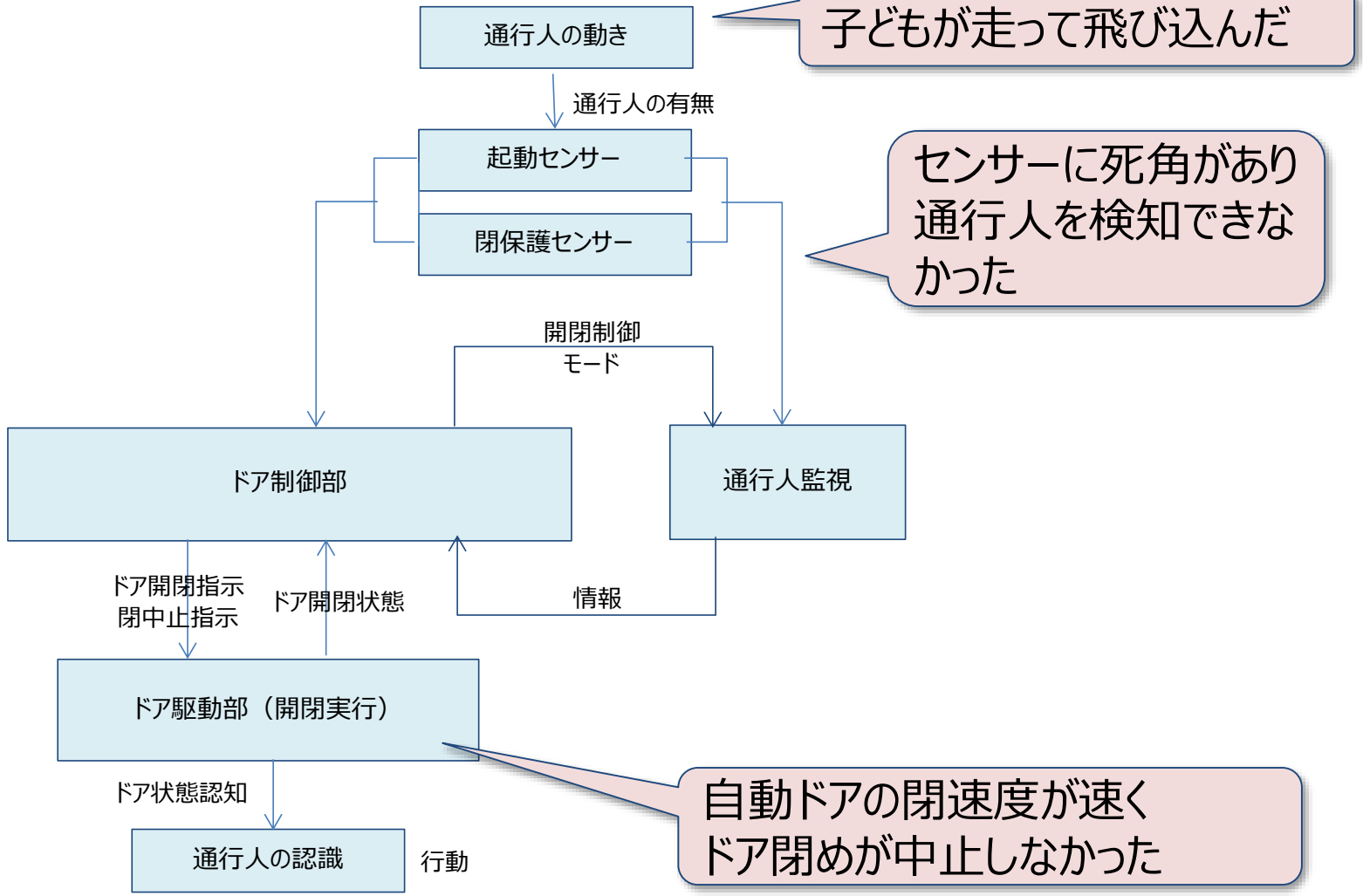
Step 0（準備2）
制御構造図の構築

Step 1
非安全な制御・指示による危険な状態につながるシナリオ分析

Step 2
危険な状態につながる要因の識別

対策検討

Step2.
ソフトウェア、人間、外部システム、環境に起因する要因として、あるべき状態と矛盾することで起きる要因を識別する



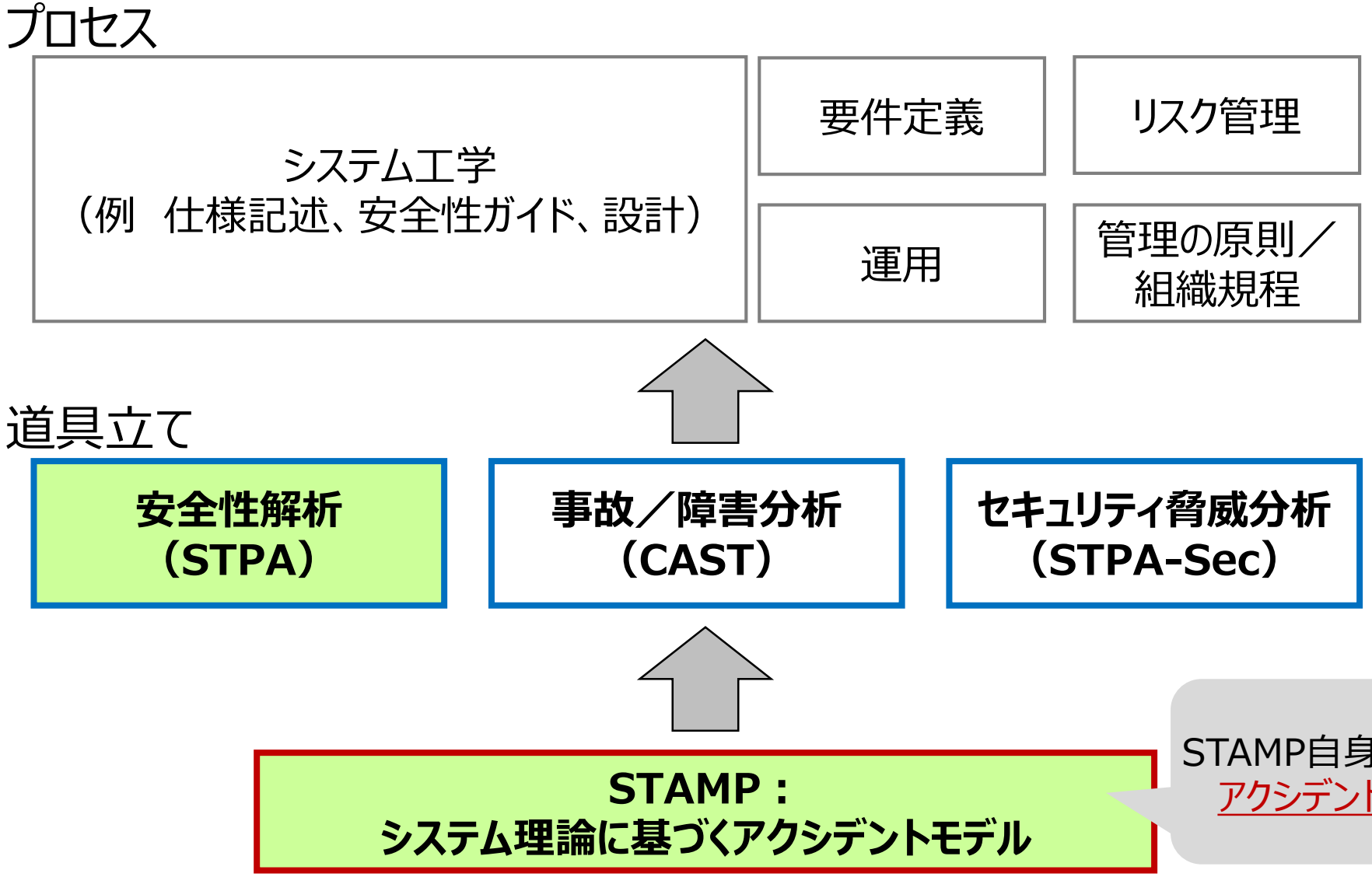
FUJITSU

STAMP/STPAの提唱者であるマサチューセッツ工科大学（MIT） 教授の
Nancy Leveson氏は、

STAMPを「説明のためのモデル（Explanatory model）」と呼んでいる

STPAは、「システムなどの発展に伴い、トップダウンのアプローチで繰り返し
行われるものである」としている

STAMPに基づく分析の道具立てとプロセス



図出典）An STPA Primer, http://psas.scripts.mit.edu/home/wp-content/uploads/2015/06/STPA-Primer-v1.pdf

FUJITSU

開発SEが使える！　今注目のリスク分析手法STAMP/STPAのシステム開発への適用

～　システム開発でのSTAMP/STPAの実践を通じて得られたテーラリングのエッセンス　～

- 何が課題か
- 何を改善したいか
- STAMP/STPA とは
- どのような方法をとったのか
- 効果は何か　どのような成果が得られたか
- 残存課題

FUJITSU

当社主催のSTAMP/STPAセミナーやワークショップに参加した技術者の声

- 「用語が難しい」
- 「導入書を読んでも分からない」
- 「どこまで分析をしたらよいか分からない」

もともと　STAMP/STPAは、
主に動的システムの安全性解析手法として、安全性を重視する
航空宇宙や自動車分野を中心に導入が進んできたため、

静的システムの開発におけるリスク分析に適した
道具立てやプロセスのテーラリングが出来ていない
ことが原因 と考察

STAMP/STPAのオリジナル手順の３つの壁

FUJITSU

- ✓ **固有の用語が多く 言葉の理解で難航**
- ✓ **「コンポーネント間の相互作用」が直感的に分かりづらい**
- ✓ **分析対象の範囲の特定が手順に書かれていない**

オリジナル手順の３つの壁
解決に導いた改善策

STAMP/STPAのオリジナル手順の**一つ目の壁**

✓ 固有の用語が多く 言葉の理解で難航

多くの技術者まず言葉の理解で難航する

分析手順の目的や意図が用語から汲み取ることができず、

「それが正しい理解なのか確証が持てない」まま分析を進め手詰まりとなる

改善策①：用語の再定義

【効果】
用語のオリジナルの定義があることを前提に対象システムで意味することを導くことができる
用語の意味を明らかにすることにつながり、比較的意味の共有感覚が得られやすい

改善策①：用語の再定義

Step 0（準備1）
損失(アクシデント), 危険な状態(ハザード), 安全制約の識別

↓

Step 0（準備2）
制御構造図の構築

↓

Step 1
非安全な制御・指示による危険な状態につながるシナリオ分析

↓

Step 2
危険な状態につながる要因の識別

↓

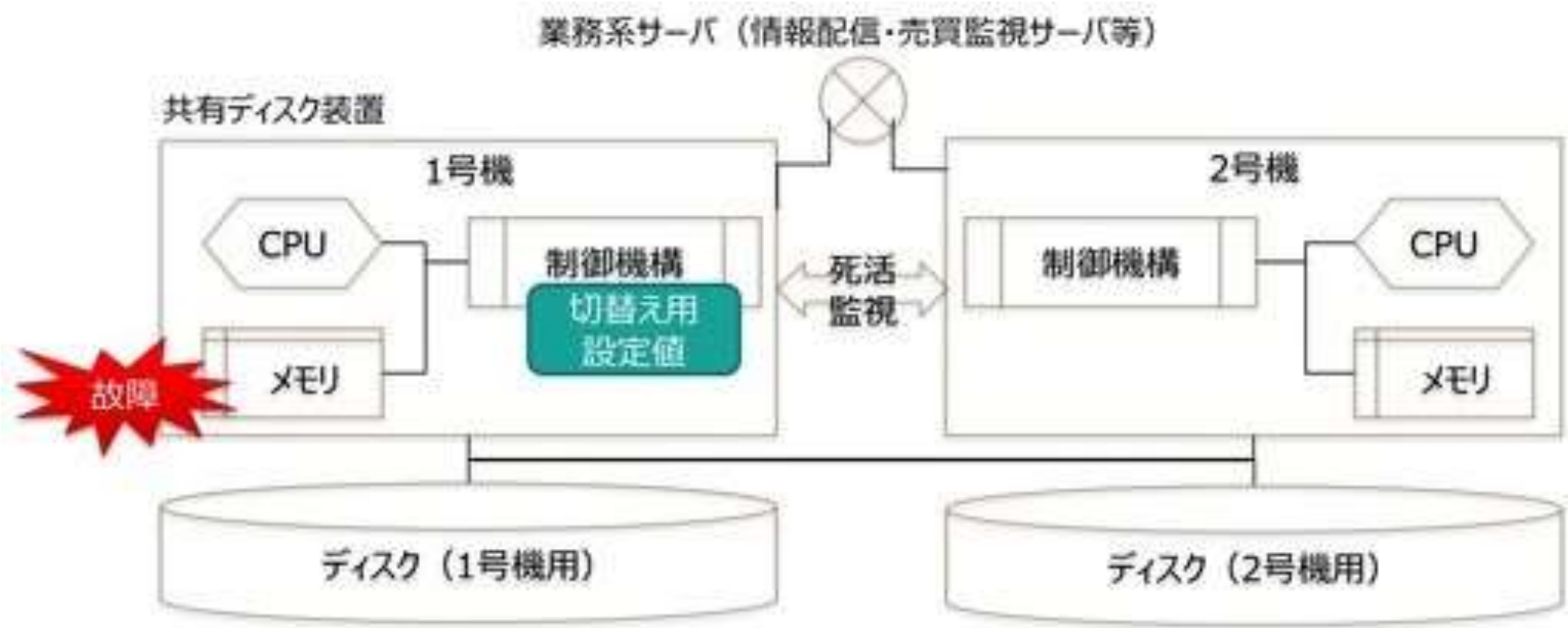
対策検討

改善策①：用語の再定義

【オリジナルの定義】

アクシデント：望んでいないし計画もしていない、損失（生命、財産、ミッション）につながるイベント

ハザード：システムを取り巻く環境が最悪な条件と重なることで、アクシデントにつながる状態

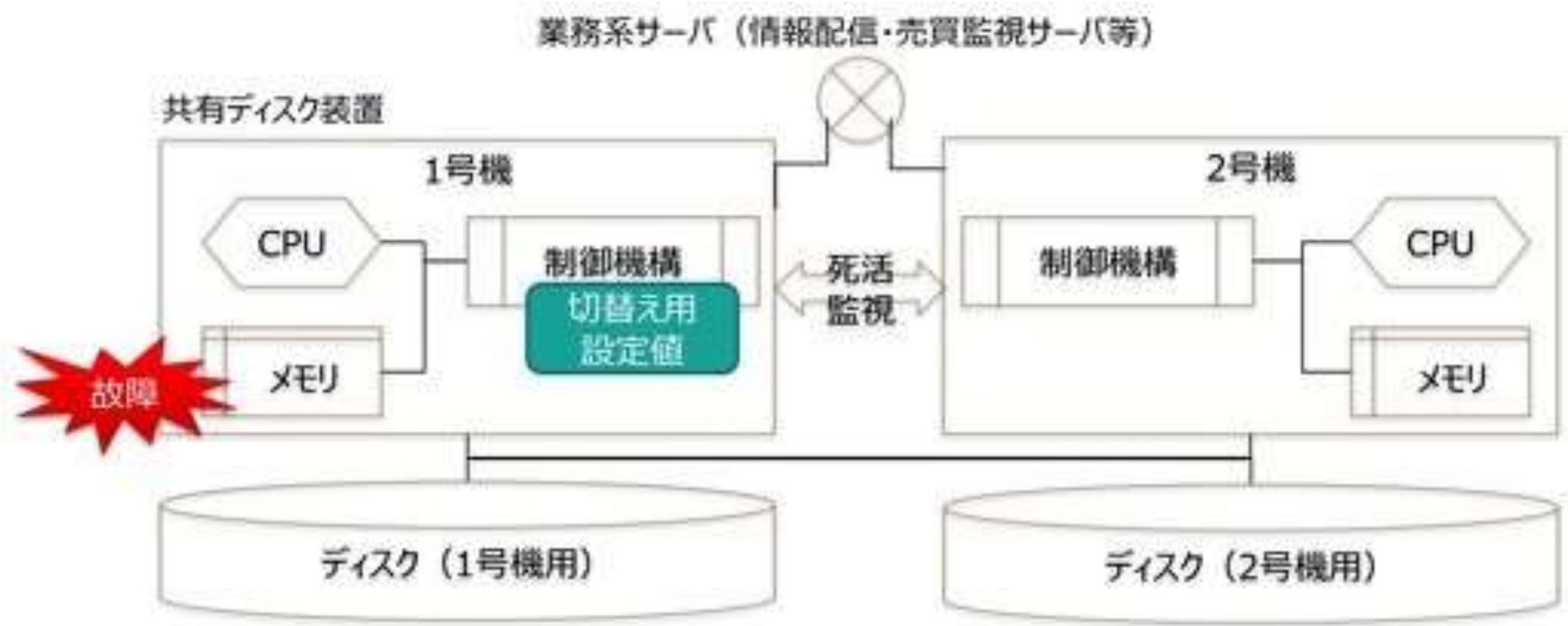


改善策①：用語の再定義

【分析対象に合わせた用語の再定義】

アクシデント：重大障害、回避すべき損失

ハザード：システムにとって危険な状態

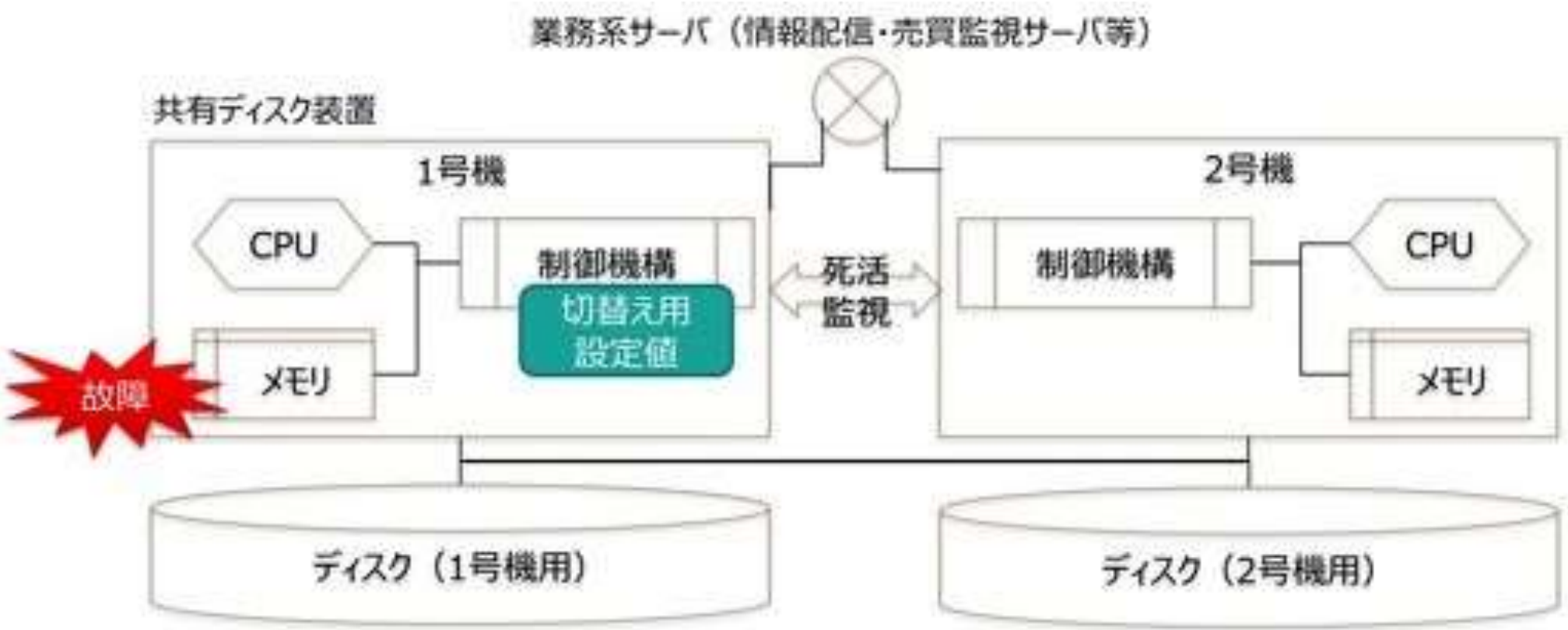


改善策①：用語の再定義

【分析対象に合わせた用語の再定義】

アクシデント：重大障害、回避すべき損失　→ 売買機会の損失

ハザード：システムにとって危険な状態　→ 送信されるべき情報が配信できない



改善策①：用語の再定義

FUJITSU

STAMP/STPA用語の再定義の例

オリジナルの用語定義と併記する

用語	オリジナルの定義	○○システム（分析対象）における意味
アクシデント	望んでもいないし計画もしていない、損失につながるようなイベント	重大障害／回避すべき損失
ハザード	システムを取り巻く環境が最悪な条件と重なることで、アクシデントにつながる状態	システムにとって危険な状態
UCA	非安全なコントロールアクション	ある条件下で重大障害につながるような指示や制御
HCF	ハザード誘発要因	危険な状態を引き起こす原因、インシデントの原因

【効果】

用語のオリジナルの定義があることを前提に対象システムで意味することを導くことができる

用語の意味を明らかにすることにつながり、比較的意味の共有感覚が得られやすい

STAMP/STPAのオリジナル手順の**二つ目の壁**

FUJITSU

✓ 「コンポーネント間の相互作用」が直感的に分かりづらい

システム構成機器を組み合わせたものをシステム全体と捉えて分析していた

従来の手法とは視点が異なるため、STAMP初心者は難しく考えてしまい、

具体的な分析対象の制御構造がどうなるかイメージすることができない

改善策②：静的システムに適合した相互作用モデルを提供

静的システムに適合した基本モデルを参照し組み合わせるイメージで御構造図が容易に作成できる

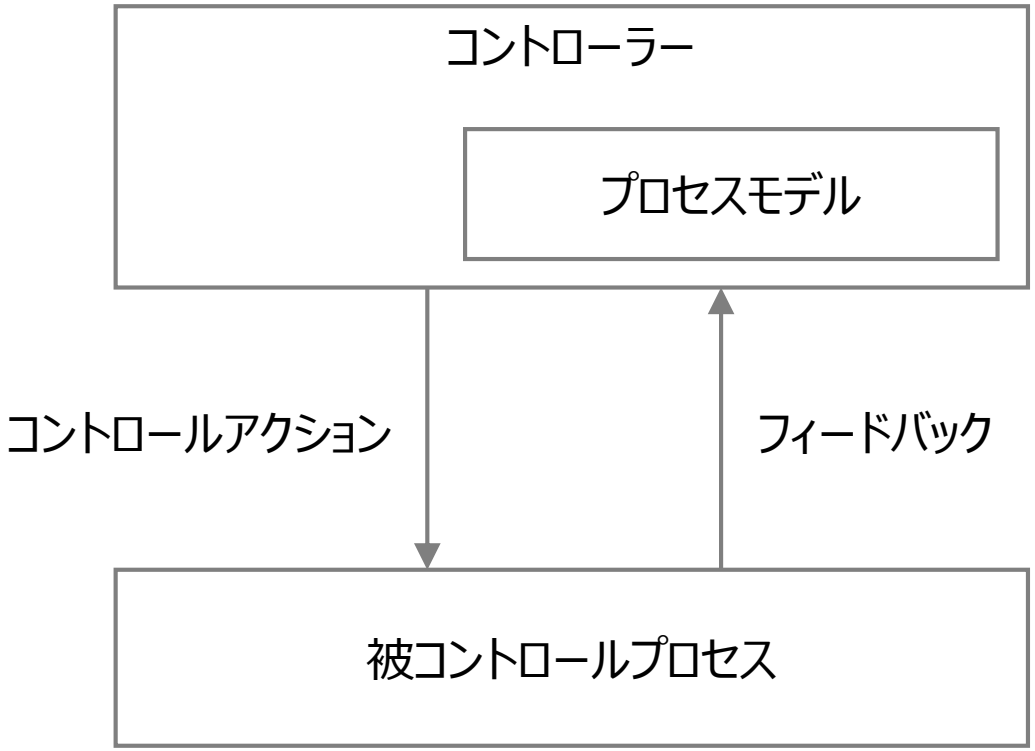
【効果】 技術者の経験や作図センスの違いによるばらつきが少なく制御構造図が構築できる

改善策②：静的システムに適合した相互作用モデルを提供

FUJITSU

オリジナルでは、コントロールアクションとフィードバックという制御系の相互作用モデルのみ提供されているため直感的に分かりづらいが、システムの仕組みをうまくグラフィカルにモデルとして表現できるため、相互作用モデルの本質的な構造は変えない

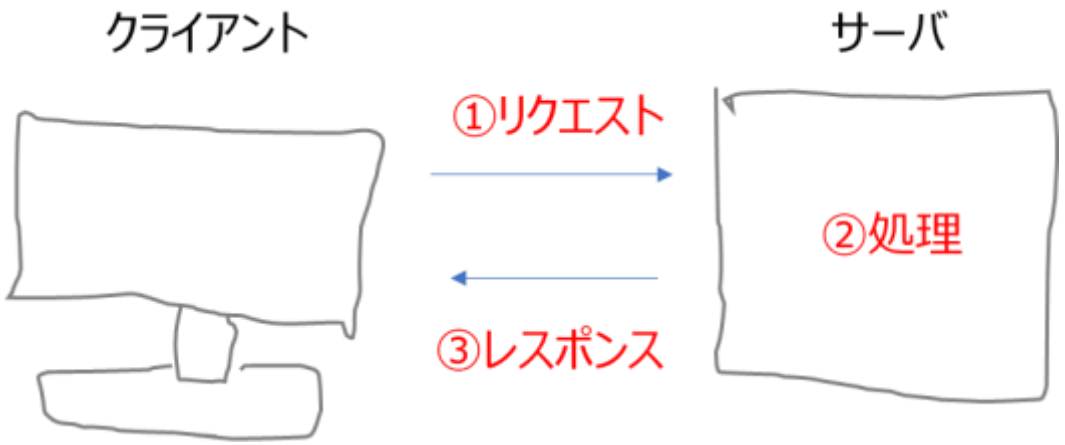
STAMPオリジナルの相互作用モデル



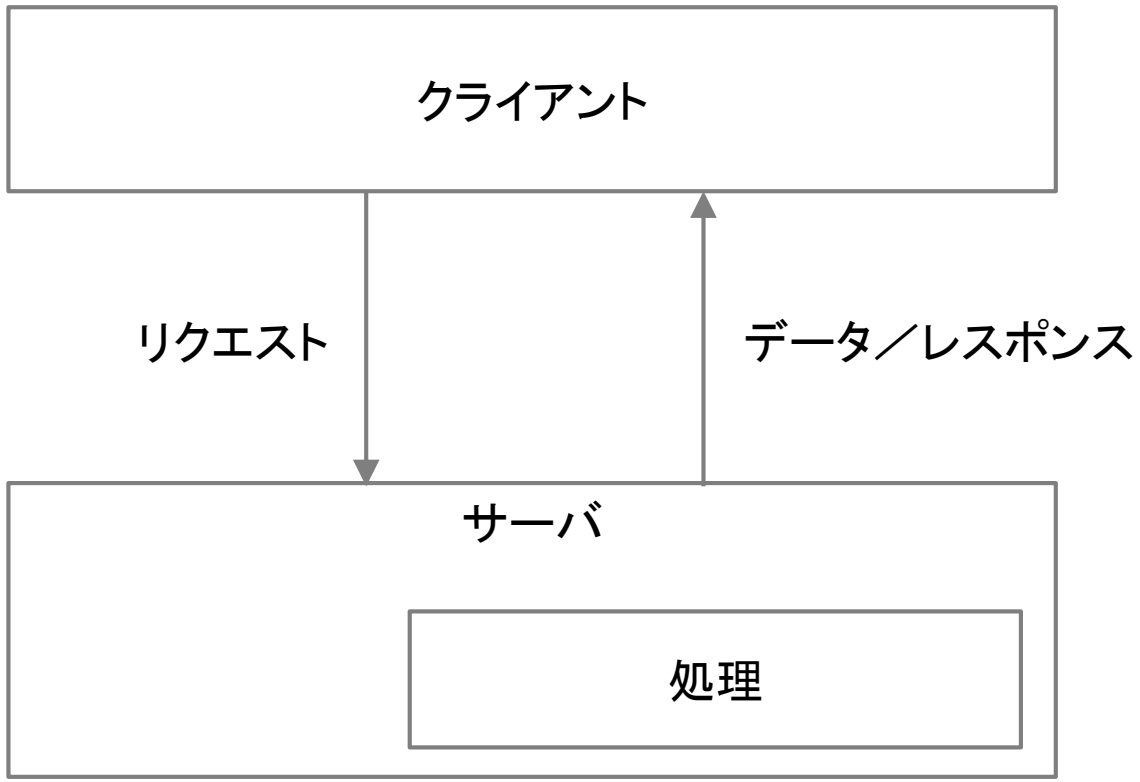
改善策②：静的システムに適合した相互作用モデルを提供

FUJITSU

「サーバクライアント」の相互作用モデルの例



オリジナルの相互作用モデル
の本質的な構造は変えない

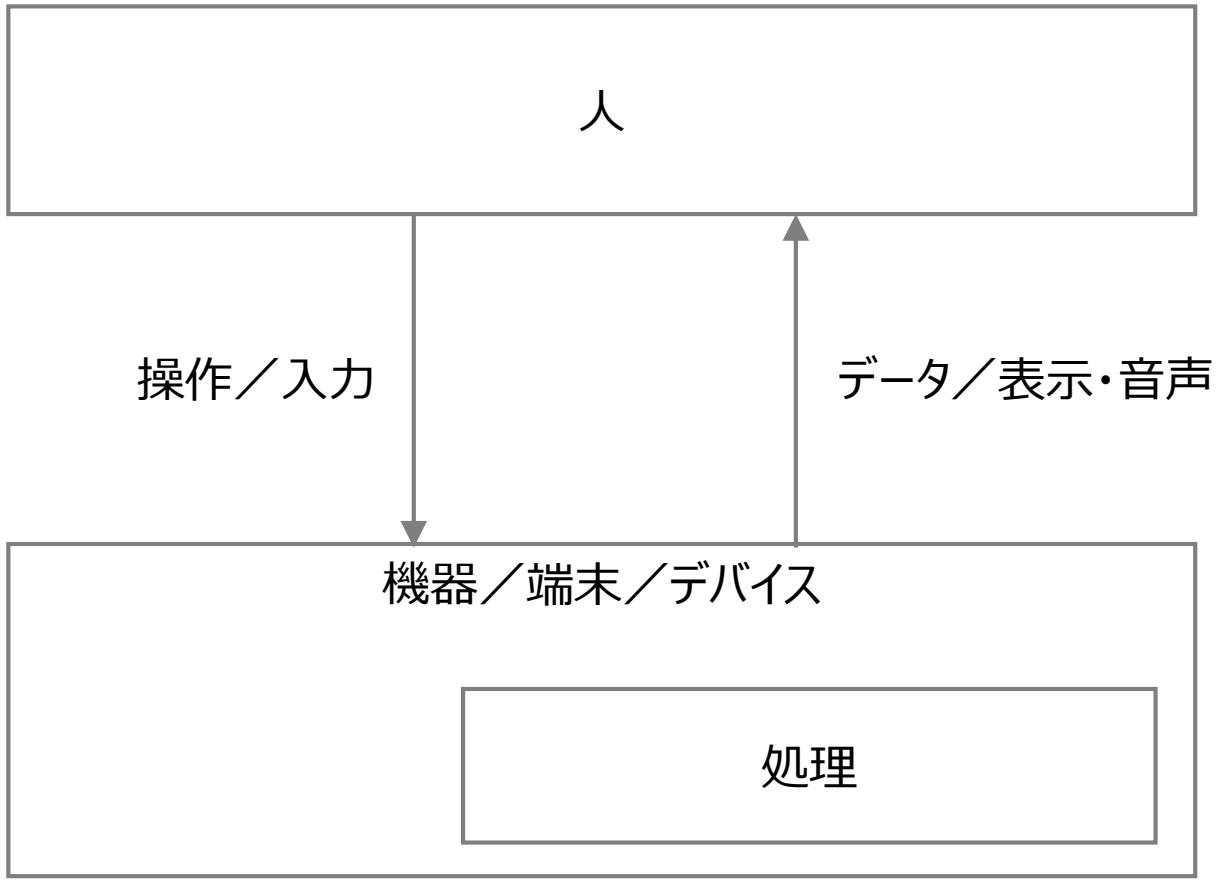


改善策②：静的システムに適合した相互作用モデルを提供

FUJITSU

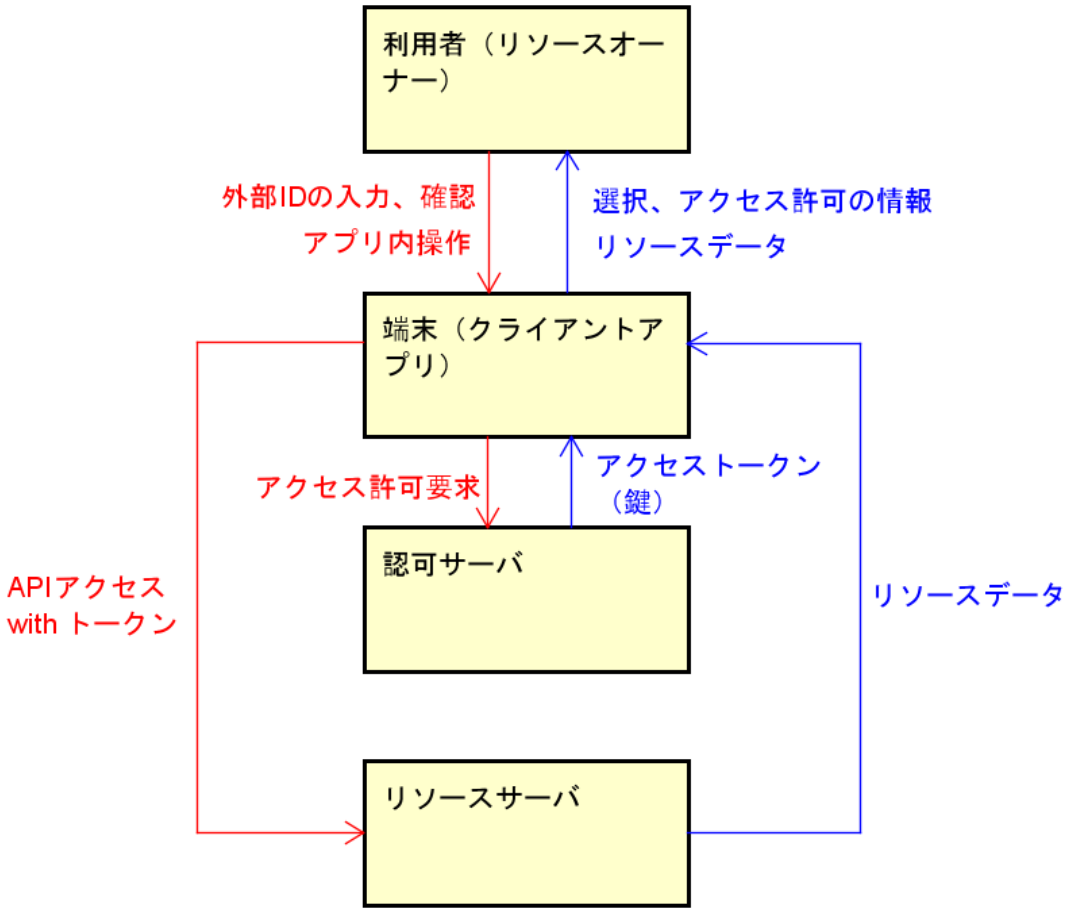
「人対機械」の相互作用モデルの例

オリジナルの相互作用モデル
の本質的な構造は変えない



改善策②：静的システムに適合した相互作用モデルを提供

新たに定義した相互作用モデルを用いた制御構造図の例



【効果】 技術者の経験や作図センスの違いによるばらつきが少なく制御構造図が構築できる

FUJITSU

✓ 分析対象の範囲の特定が手順に書かれていない

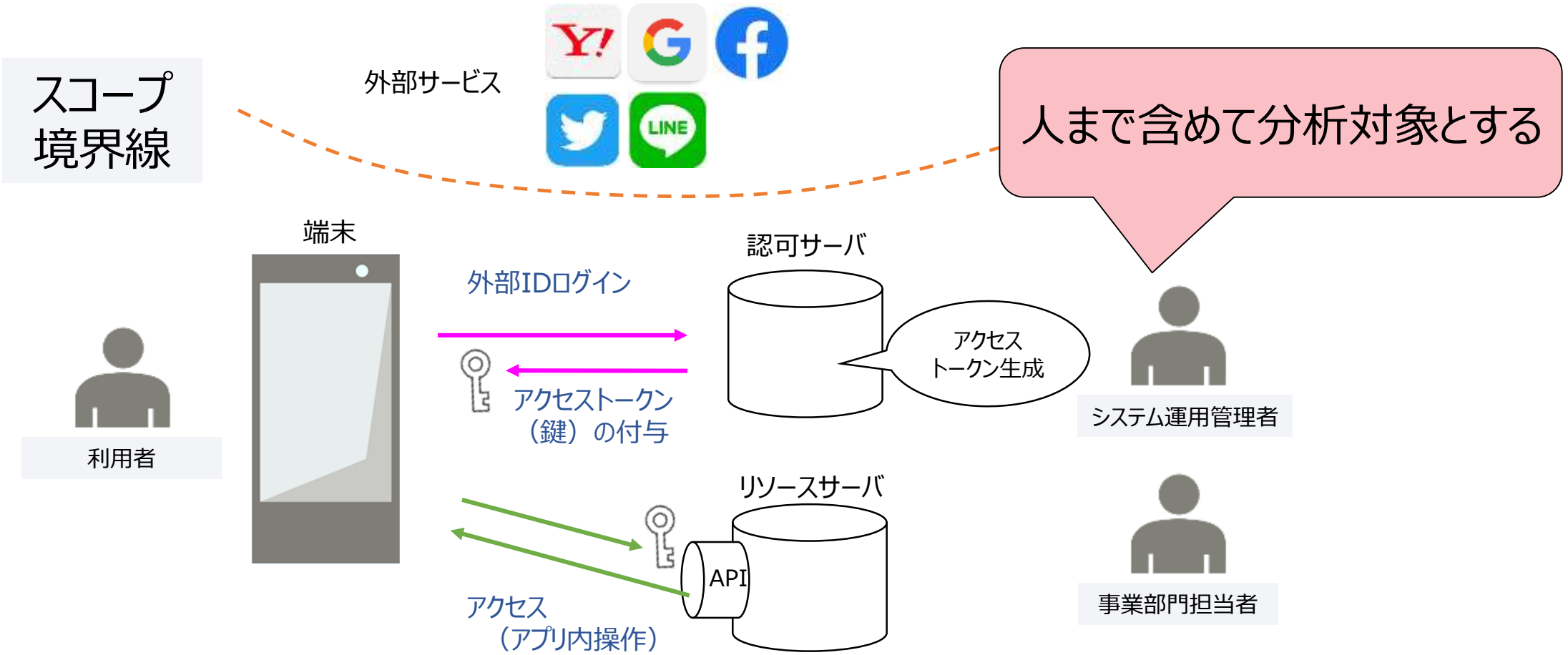
オリジナルの定義では、システムの境界を定めず分析可能な範囲を拡げるといった意図があり、
実施手順には「分析対象の範囲（Scope）の特定」が書かれていない
その結果、「風が吹けば桶屋が儲かる」的に範囲を際限なく広げなければならないのか
と懸念し、どこまで作業すればよいのかわからず悩むことになる

改善策③：登場人物の配置で分析対象の境界を規定

【効果】 システムの境界を定めず分析可能な範囲を拡げるといったSTAMP/STPAの意図を損なわず分析範囲を明確にできる。 分析を進めていく中で度々起こる関係者間での分析範囲の「ゆらぎ」が少なくなる

改善策③：登場人物の配置で分析対象の境界を規定

人を含むシステム全体のポンチ絵を描いて、分析範囲を決定する



【効果】 STAMP/STPAの意図を損なわず分析範囲を明確にできる。
分析を進めていく中で度々起こる関係者間での分析範囲の「ゆらぎ」が少なくなる

開発SEが使える！　今注目のリスク分析手法STAMP/STPAのシステム開発への適用

～　システム開発でのSTAMP/STPAの実践を通じて得られたテーラリングのエッセンス　～

- 何が課題か
- 何を改善したいか
- STAMP/STPA とは
- どのような方法をとったのか
- **効果は何か　どのような成果が得られたか**
- 残存課題

改善策を適用して実施した分析の概要

FUJITSU

項目	内容
分析対象	○○システム開発プロジェクト（静的システム）
分析者	6名（STAMP初心者）（注1）
工数	1.5人日（注2）
モデリングツール	STAMP Workbench（注3）

（注1）分析者は、システム開発でSTAMP/STPAを実践するのは初めて
（注2）分析は対策立案まで含めて個人ワークとし、分析者1名あたりの実施工数
（注3）独立行政法人情報処理推進機構 社会基盤センター.
“STAMP向けモデリングツールSTAMP Workbench”

STAMP初心者による分析の結果

FUJITSU

分析の結果（成果）	抽出件数（※）
「危険な状態につながるシナリオ」抽出件数	７１
新たな「設計考慮漏れ」が見つかった件数	6
考慮漏れのうち、「対策が必要」と判断されたリスク項目	4
コストダウン、生産性向上につながる改善施策の導出件数	1

（※）分析者6名が抽出した総件数（重複分除く）

改善策による効果検証

一回目：STAMP/STPAオリジナルの説明と手順で簡単な事例で分析を実施
二回目：改善策を実際のプロジェクトに適用して分析を実施
各分析後にとったアンケートの5段階評価結果を基に理解度、有用度を指数化した結果

	改善前	改善後	
STAMP/STPAの理解度	4.00	⇒ 4.33	
STAMP/STPAを使った自律的な分析ができる	3.83	⇒ 4.67	
分析手順や道具立ての分かりやすさ	3.80	⇒ 4.67	
STAMP/STPAの業務への役立ち度	3.60	⇒ 4.83	

成果まとめ

- STAMP初心者が自律的な分析を実施し、リスク要因を抽出し、障害の未然防止につながる対策を設計に織り込むことが出来ることを確認した
- さらに、お客様の経営目的（コストダウン、生産性向上）につながる施策を導出するツールとしても活用できる可能性を見出した

FUJITSU

開発SEが使える！　今注目のリスク分析手法STAMP/STPAのシステム開発への適用

～ システム開発でのSTAMP/STPAの実践を通じて得られたテーラリングのエッセンス　～

- 何が課題か
- 何を改善したいか
- STAMP/STPA とは
- どのような方法をとったのか
- 効果は何か　どのような成果が得られたか
- **残存課題**

残存課題

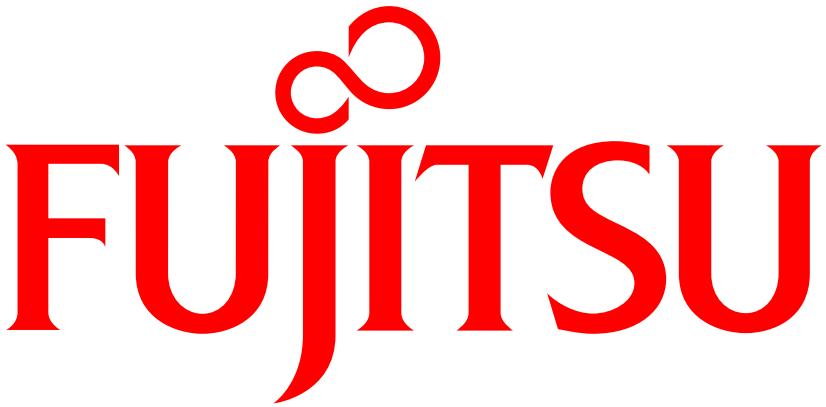
FUJITSU

- 障害が起こる条件の抽出やそれらの要因抽出のばらつきや偏り

  発想を強制的に引き出し、障害シナリオを網羅的に抽出できるようにするためのSTAMP/STPAの道具立てのひとつであるガイドワードの改良

- STAMP/STPAは、自然言語を用いて障害シナリオを抽出する手法であり、残存リスクを定量的に評価しない

  抽出したリスク要因に対して、発生確率と影響度といった指標で残存リスクを定量的に評価する取り組みも必要



shaping tomorrow with you