安全工学由来のモデリングSTAMPを用いた大学院PSP教育改善活動の促進

日下部 茂*，梅田 政信，片峯 恵一，荒木俊輔
九州工業大学(*投稿時は長崎県立大学)

2023年10月12日

アウトライン

- はじめに
- 動機づけモデル(既存の改善活動の一部)
- STAMP/STPA(上記を促進)
- 質的アプローチ/CAST(失敗事例から学ぶ)
- おわりに

プロセスの教育

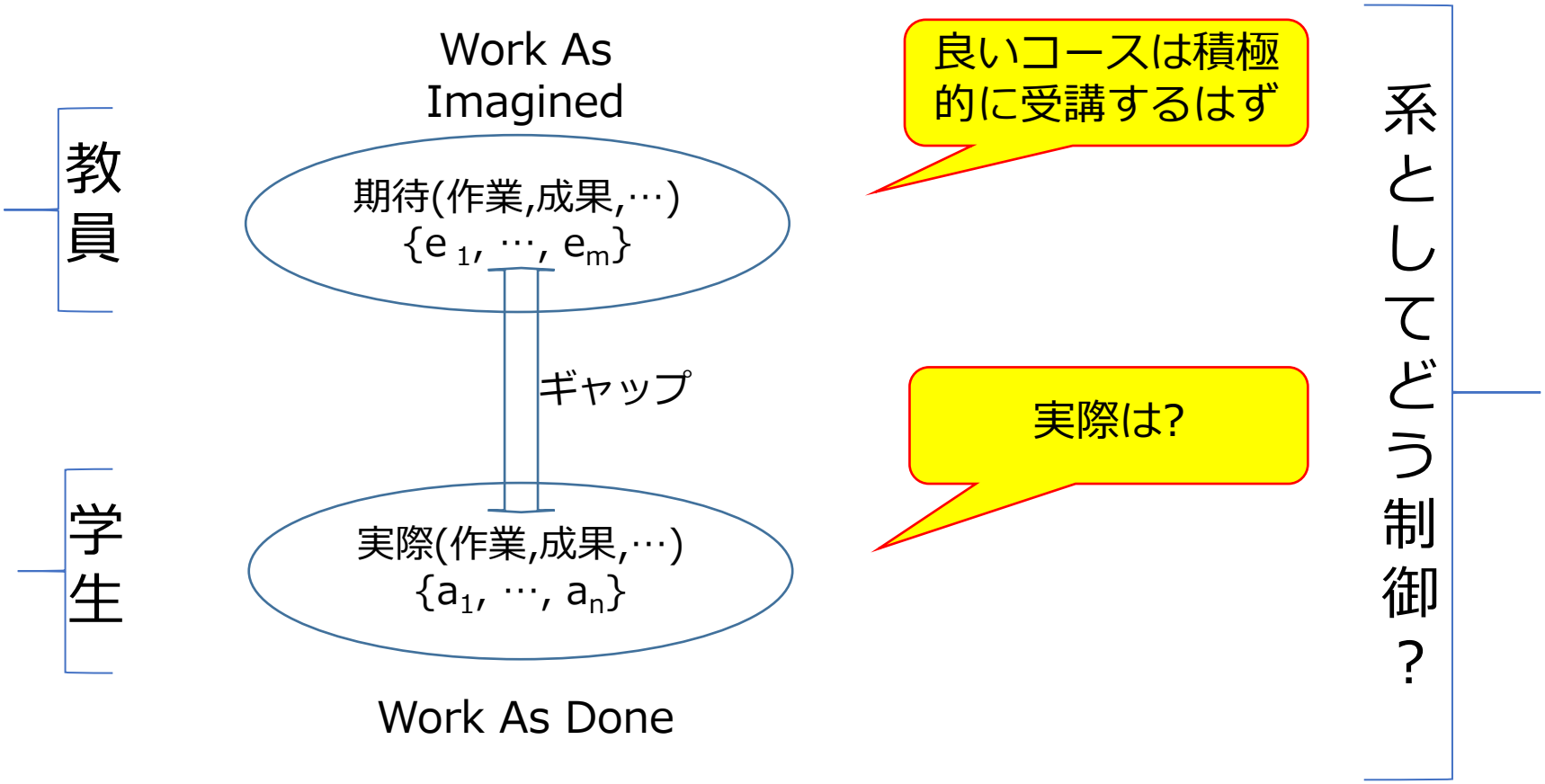
- ソフトウェアの比重拡大
  →その調達や開発における品質管理
  - ビジネスの成功や安心・安全な社会を実現する上で必須
- ソフトウェア開発＝知識作業
  - 作業者の頭の中での作業
  - タスクマネジメント　⇒　知識作業マネジメント
- 高品質ソフトウェアを計画や予算内で開発できる技術力, チーム力, マネジメント力：プロセス教育
- 個人：Personal Software Process (PSP)
  - ソフトウェア技術者のための継続的自己改善手法
- チーム：Team Software Process (TSP)
  - 自律チームの構築とマネジメント

プロセス(PSP)実習講義の成果と課題

九州工業大学・大学院(以降,九工大)での実施事例

- 規模と時間の見積り
  - 見積り誤差が減少し、＋/ーに程良くバランスする傾向
- 製品の品質
  - プロセス欠陥除去率 >= 約60%
  - 50欠陥/KLOC → 10欠陥/KLOC
- 生産性
  - コースの前後でほぼ同じ
- コースの修了率
  - PSP-Planningは2010年以降はほぼ 100%
  - PSP-Qualityは20%程度（＝＜　社会人50%程度）

PSP教育の改善にシステム思考



PSPコース未修了の原因

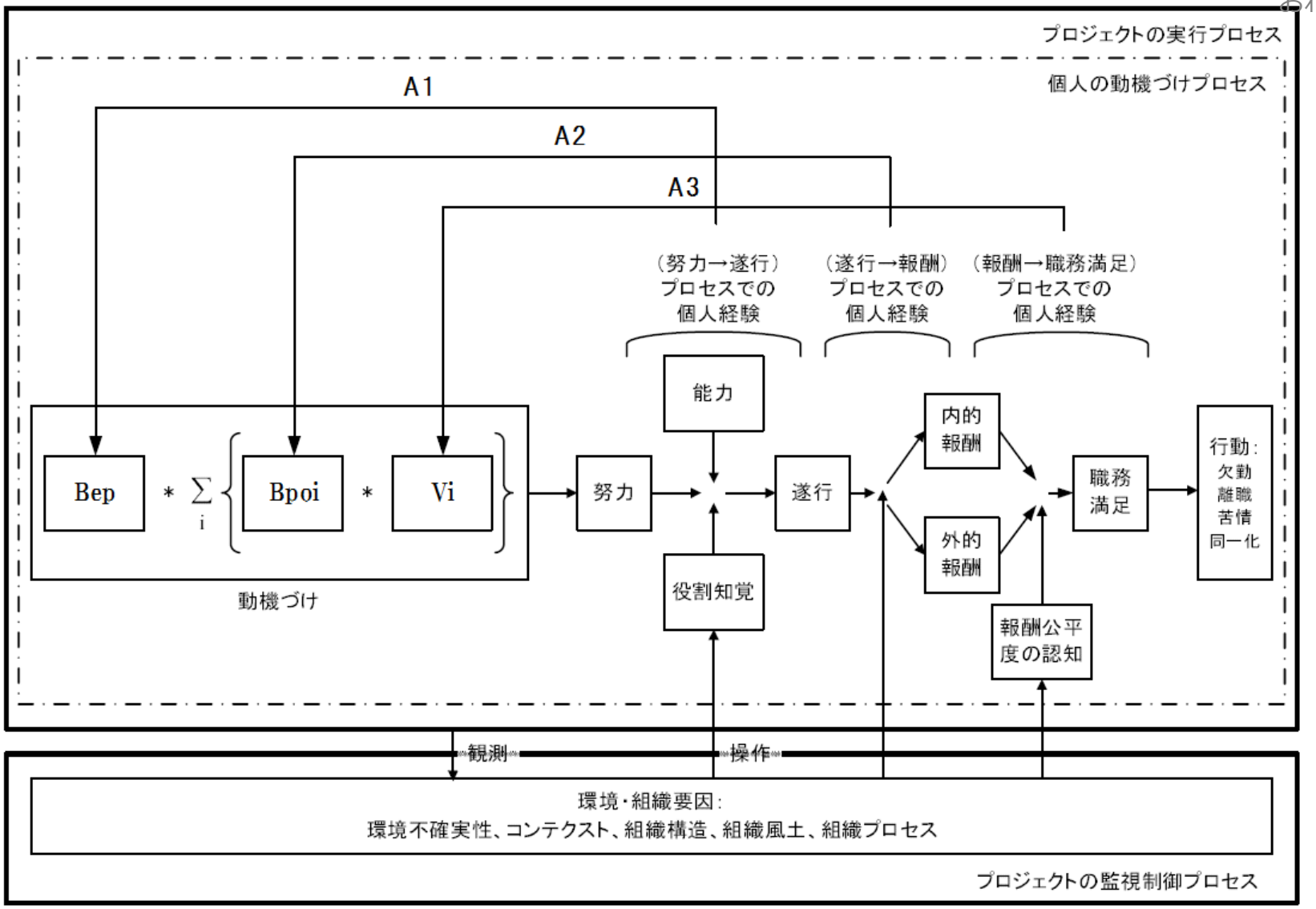
- プログラミングスキルの不足
  - ガイダンスの充実により解消
- 大きい演習負荷
  - （講義3時間＋演習課題/レポート平均7時間）×10回
- 時間管理スキルの不足
  - 研究活動との両立困難
- 動機づけが重要
  - 一般にも新しい技術や手法の導入，定着に必要
  - 動機づけに関わる指導方法は経験とカン？

- PSPコースにおける動機づけプロセスの定式化
- 効果的で効率的なPSPコース運用方法の確立

動機づけに関する関連研究

- 動機づけ理論
  - 内容理論、過程理論など
- 動機づけの期待モデル(Lawler,1971)
  - 動機づけのプロセス
- 組織論的期待モデル(坂下,1981)
  - 個人の動機づけプロセスと環境や組織の要因との関係
- 動機づけプロセスの状態遷移モデル(石橋ら,2013)
  - 技術や手法の導入におけるプロセスの分析に有効
  - PSPコースへの適用法は自己学習のモデルで不完全

動機づけプロセスとその構造

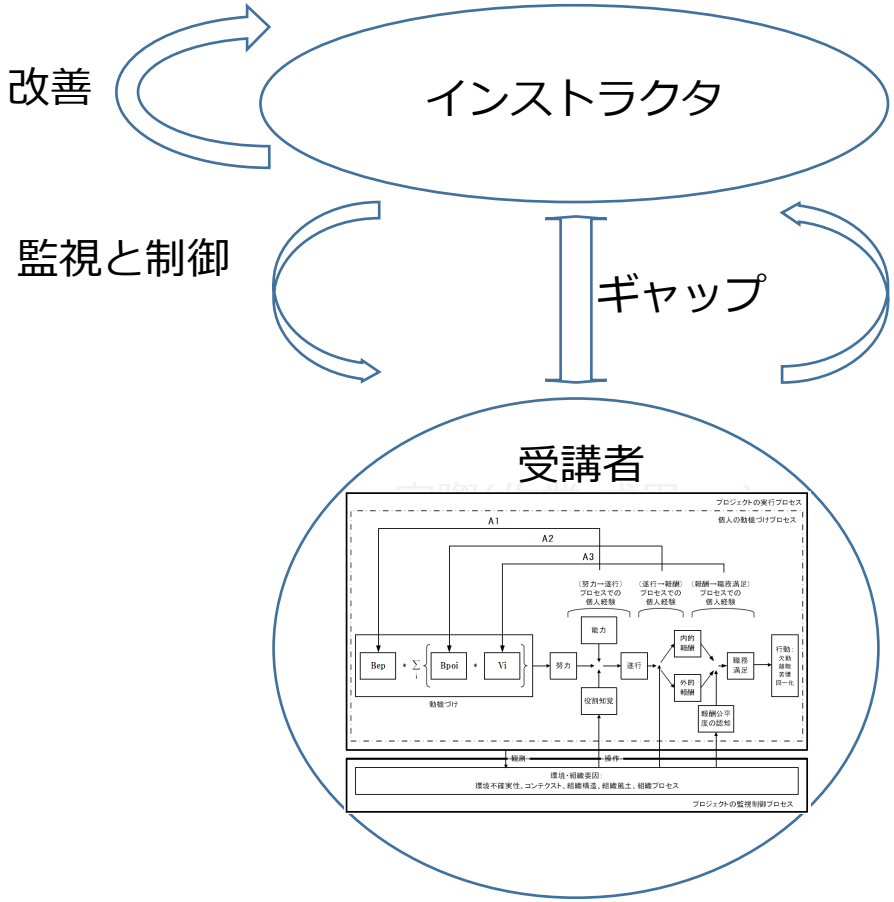


動機づけプロセスの状態遷移モデル

- 状態遷移モデル
  - 個人や組織を一つの状態機械と見なす
  - プロセスの状態とそれに対する操作により動機づけプロセスを定式化
- 状態集合
  - 要因fの状態S_fは有意な範囲で離散化可能とする
- 操作集合
  - 操作は，役割知覚，遂行に対する報酬，報酬公平度の認知に影響を与える行為
    - ✓例：技術の重要性を説明する、遂行のレベルをほめる
- 状態遷移
  - 状態遷移は非決定性 (確率的に遷移)
- シナリオ
  - 初期状態S_0から最終状態S_nに至る状態の時系列
    - ✓定着成功シナリオ：技術や手法の導入成功に至るシナリオ
    - ✓定着失敗シナリオ：技術や手法の導入失敗に至るシナリオ

PSPトレーニングの指導への適用

- 動機づけ制御の構造



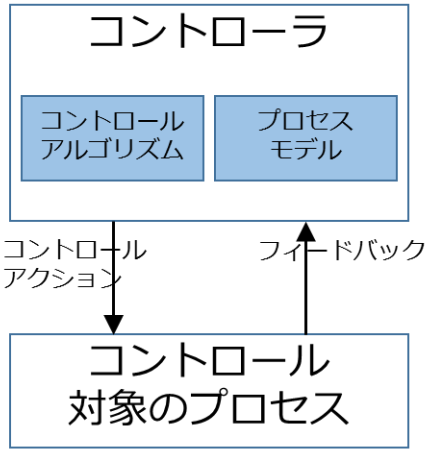
インストラクタからの動機づけの制御方法は?

受講者に動機づけモデルを使う場合,指導者は?

システム理論的因果律モデル STAMP (Systems-Theoretic Accident Model & Process)

- MIT のNancy Leveson 教授が提唱
  - SW集約システムだと従来の解析的還元論や信頼性理論には限界⇒システム理論に基づき,コンポーネント間の相互作用に着目した事故モデル

- 三つの基本モデル要素：
  - コントロールストラクチャ(CS)
    - ✓システムの構成要素間の構造と，相互作用を表したもの
  - プロセスモデル
    - ✓対象プロセスに対する抽象表現とコントロールアルゴリズム
  - 安全制約
    - ✓安全のために守るべき制約

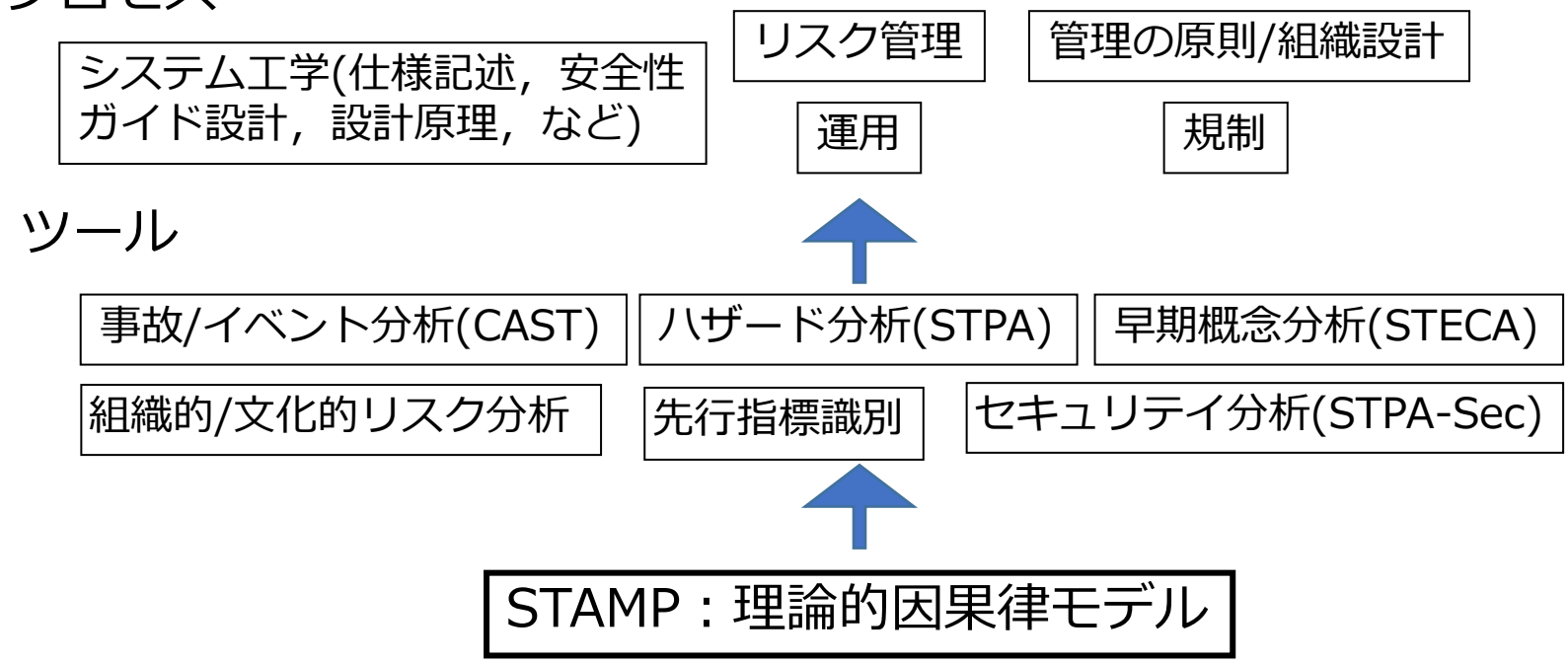


- CSとプロセスモデルに対して，システムの安全制約が正しく適用されているかどうかに着目(コントロールの問題に着目)

STAMPに基づくツールとプロセス

ソフトウェアやハードウェア，社会システムも含んだ包括的な分析が可能な事故モデル

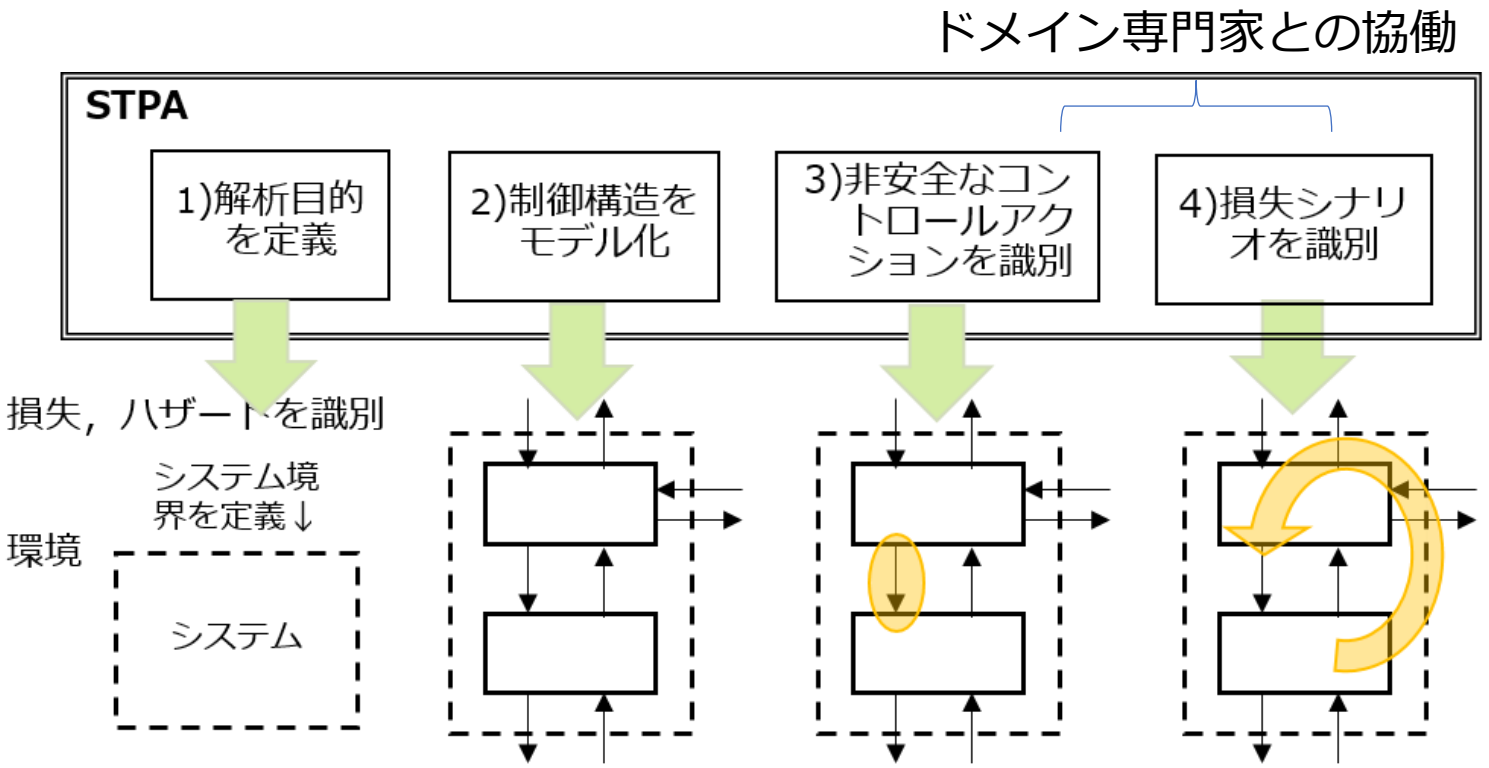
ハザード分析・事故分析手法を用いたプロセス改善分析



ハザード分析 STAMP/STPA

STPA(Systems Theoretic Process Analysis)

- トップダウンに詳細化などを繰り返し・再帰的に



九工大事例：指導方針

- SEIによるPSP修了基準(全課題完了)を満たさずコースをやめる
  - TSP/PSP報告会や産業界講師による講演といった産学連携を通じ，就職後も念頭にPSP修了の重要性と魅力を伝える
- 大学の単位修得要件(課題の2/3完了)を満たさずコースをやめる
  - 単位修得要件を明示し，単位修得を促す
- プロセスを改善できずに同じ誤りを繰り返す
  - 改善できない原因の究明の手助けをすると同時に，対応する指導を繰り返し行う
- プロセスの改善点の一般化ができない
  - 回答を与えずに，気づくまで繰り返し指導を行う
- 進捗が遅延し課題を予定通り完了できない
  - 毎回の講義開始時や事前に遅れが察知された時点で進捗を確認し，適宜(週単位で)講義日時の変更や追加説明を行う
- 分析が不十分で適切な改善提案ができない
  - 適宜気づきを促す助言を与える
- Engineeringのスキルの低さによりプロセス改善効果がでない
  - Software Engineering視点で助言を与える.

STAMP/STPA Step1

プロセス改善系(システム)には様々な要素・サブシステム.

安全制約を守れずアクシデントになり得るハザードの原因：

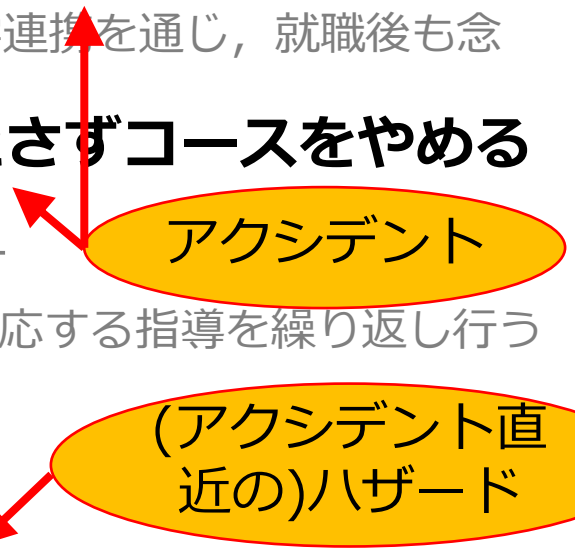
- 対処されない環境外乱や環境条件
- 対処されなかったりコントロールされなかったりするコンポーネントの障害
- コンポーネント間の非安全な相互作用
- 適切に協調されていない複数のコントローラによるコントロールアクション

開始準備を整える(Step1)

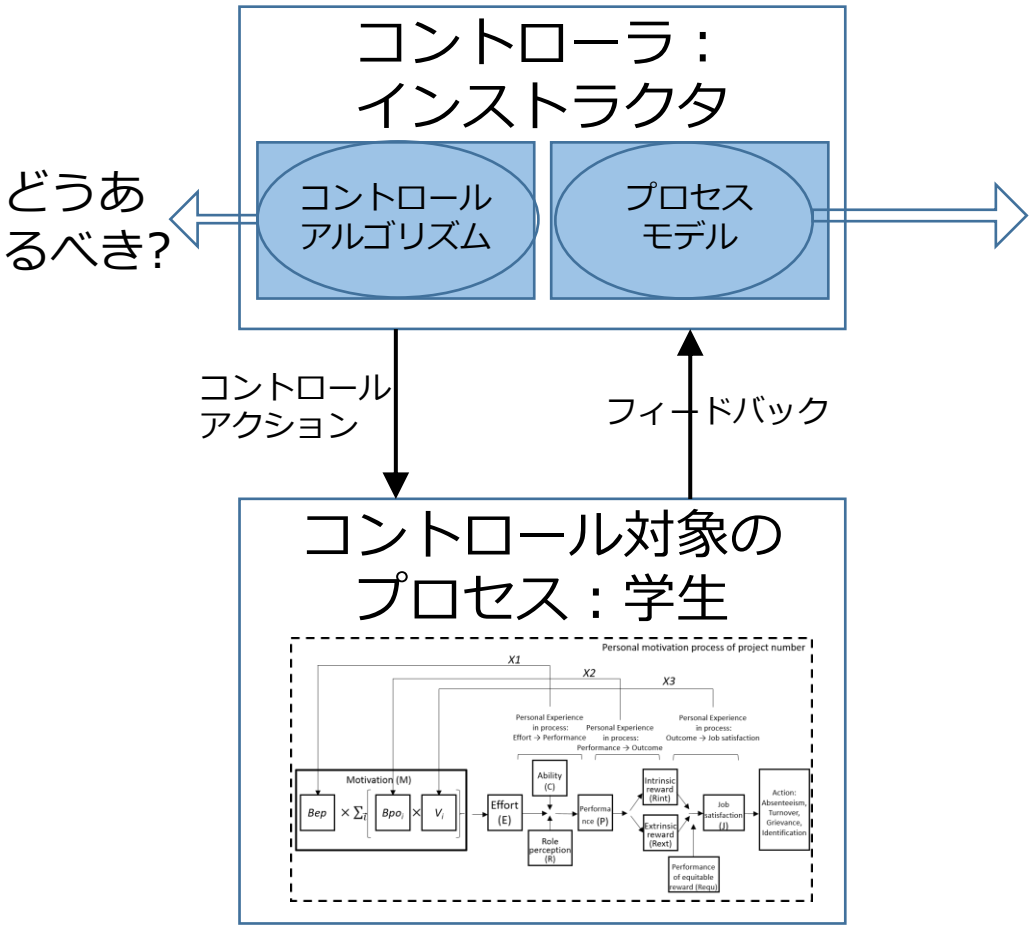
- アクシデント(損失)，ハザードの決定
- コントロールストラクチャの構築

九工大事例：Step1

- **SEIによるPSP修了基準(全課題完了)を満たさずコースをやめる**
  - TSP/PSP報告会や産業界講師による講演といった産学連携を通じ，就職後も念頭にPSP修了の重要性と魅力を伝える
- **大学の単位修得要件(課題の2/3完了)を満たさずコースをやめる**
  - 単位修得要件を明示し，単位修得を促す
- プロセスを改善できずに同じ誤りを繰り返す
  - 改善できない原因の究明の手助けをすると同時に，対応する指導を繰り返し行う
- プロセスの改善点の一般化ができない
  - 回答を与えずに，気づくまで繰り返し指導を行う
- **進捗が遅延し課題を予定通り完了できない**
  - 毎回の講義開始時や事前に遅れが察知された時点で進捗を確認し，適宜(週単位で)講義日時の変更や追加説明を行う
- 分析が不十分で適切な改善提案ができない
  - 適宜気づきを促す助言を与える
- Engineeringのスキルの低さによりプロセス改善効果がでない
  - Software Engineering視点で助言を与える.



Step2: コントロールストラクチャ

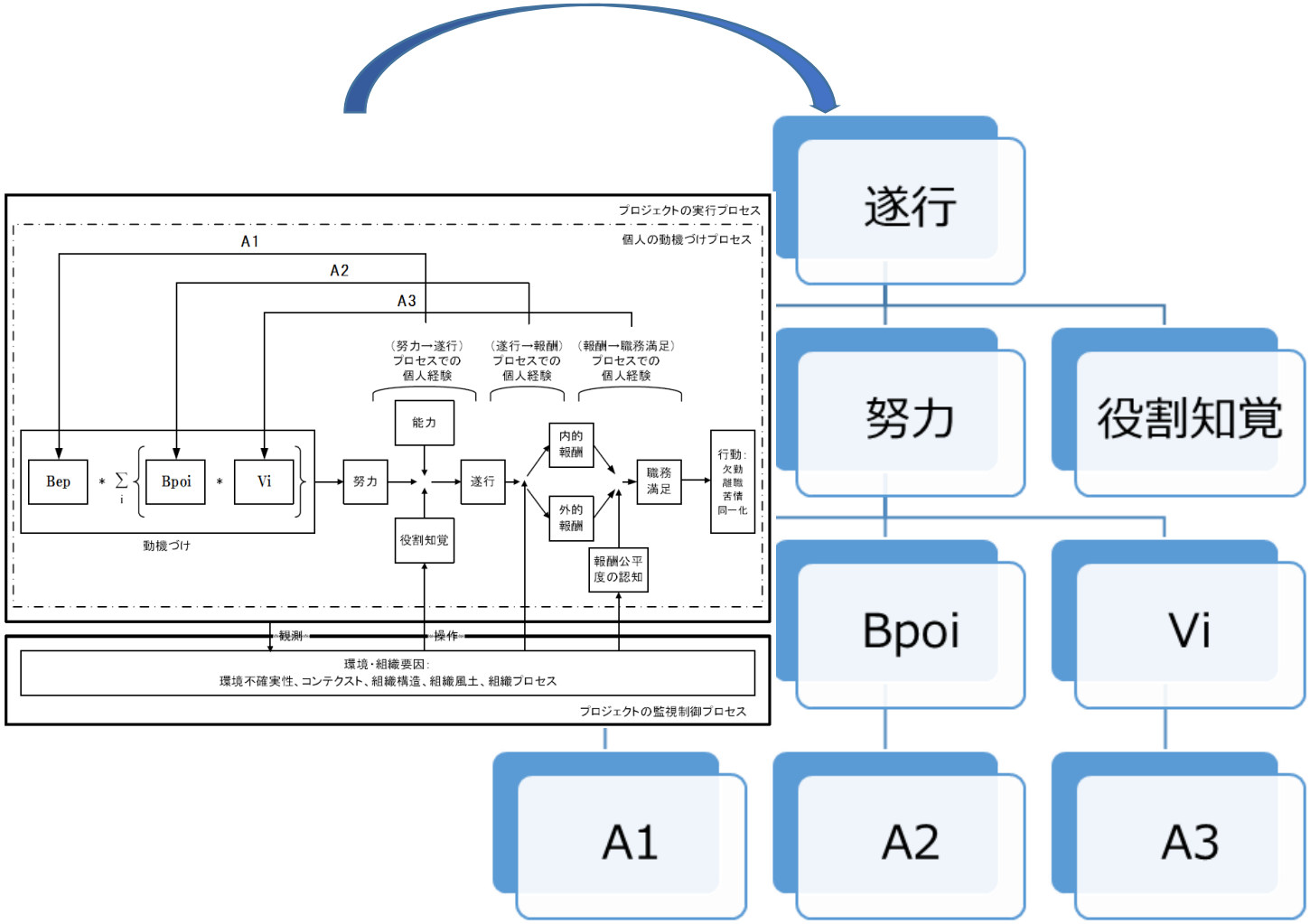


PSPコース用プロセスモデル変数

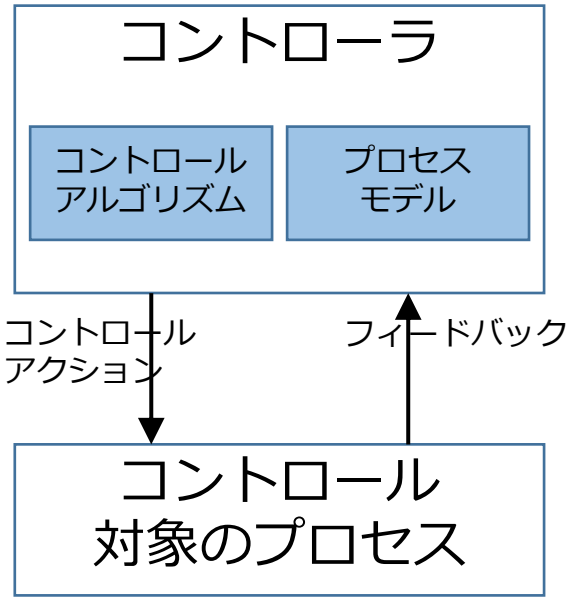
Factor	State value set
Bep	{VeryHigh, High, Low, Unknown}
Bpo	{High, Low, Unknown}
V	{High, Low, Unknown}
Effort *E*	{VeryHigh, High, Low, Unknown}
Ability *C*	{VeryHigh, High, Low, Unknown}
Role Perception *Ri* (i=1..87)	{Perceived, NotPerceived, Unknown}
Performance *Pj* (j=1..10)	{Accomplished, NotAccomplished}
Assignment *Aj* (j=1..10)	{NotGiven, Given, PlanningCompleted, Completed}
Intrinsic Reward	{Given, NotGiven}
Extrinsic Reward	{Given, NotGiven}
Job Satisfaction	{HighLevel, LowLevel}

動機づけプロセスモデルを内在

階層的制御構造への視点転換



Step3: Unsafe Control Action の識別



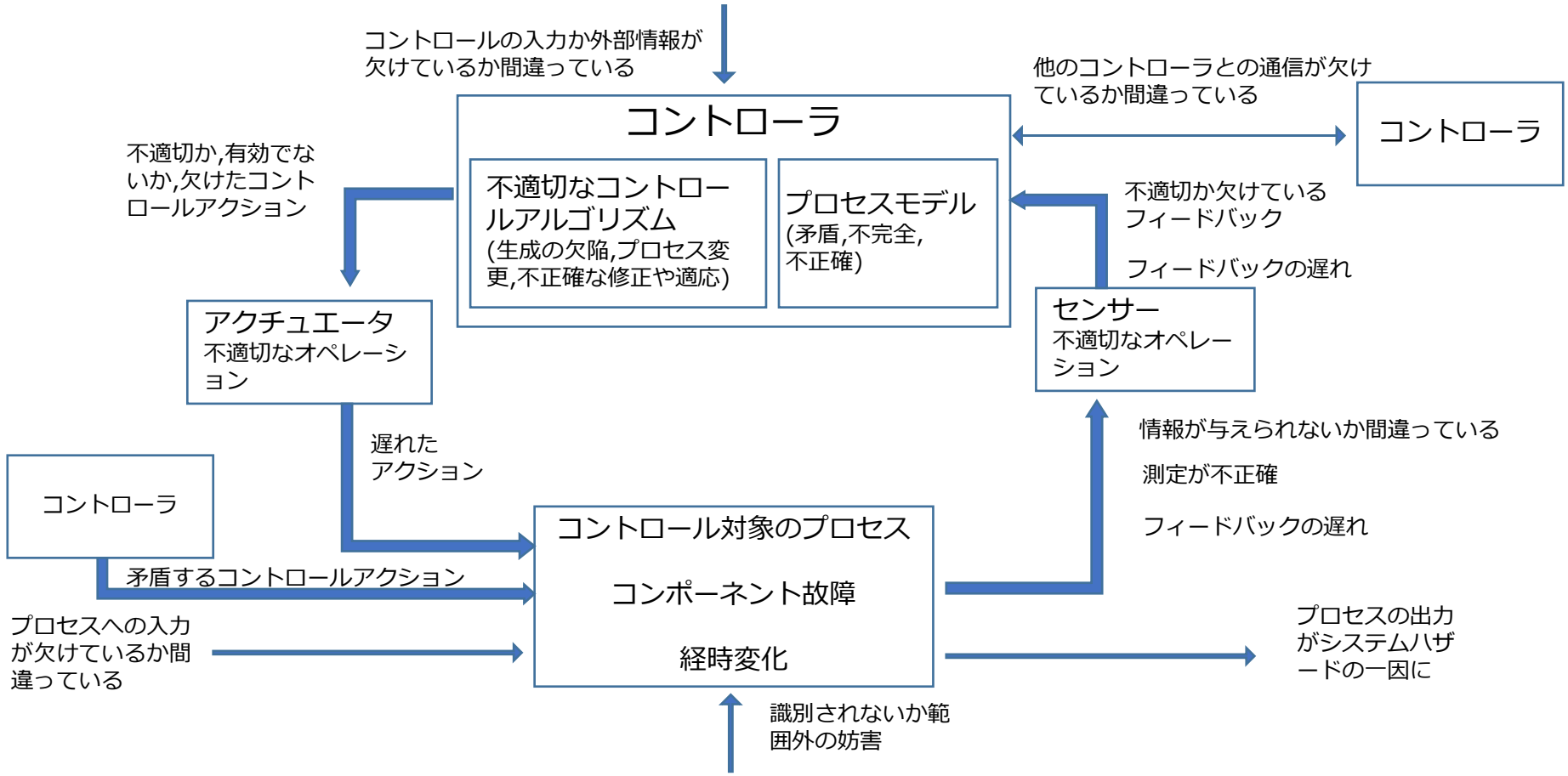
- プロセスモデルが正しくないときに事故がしばしば起きる
- 四つのタイプの非安全なコントロールアクション
  - 安全のために必要なコントロールコマンドが与えられない
  - 非安全なものが与えられる
  - 潜在的安全コマンドが早すぎ/遅すぎて与えられる
  - コントロールがすぐ止まりすぎ、長く適用されすぎ

コントロールアクション	**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、誤順序でハザード**	**早すぎる停止、長すぎる適用でハザード**
(コントロールアクション)	(条件)	(条件)	(条件)	(条件)
…	…	…	…	…

九工大事例：Step3

コントロールアクション	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,誤順序でハザード	早すぎる停止、長すぎる適用でハザード
課題提出指示	…	不適切な想定にもとづく課題提出指示	努力が遂行に結びつかない状況での課題提出指示	…
…	…	…	…	…
指導アクション$_j$	努力を遂行へつなげるのに必要な追加の指導が与えられずハザード	不適切な方法での指導のため望ましい状態遷移が起きずにハザード	準備ができていない時期の指導，時期を逸した指導，誤順序の指導などでハザード	継続的実施の必要がある遂行に関する指導を早くやめすぎるなどでハザード
…	…	…	…	…

Step4: 損失シナリオの識別(適宜置換え)



動機づけプロセスの状態遷移モデル

- 状態遷移モデル
  - 個人や組織を一つの状態機械と見なす
  - プロセスの状態とそれに対する操作により動機づけプロセスを定式化
- 状態集合
  - 要因fの状態S_fは有意な範囲で離散化可能とする
- 操作集合
  - 操作は，役割知覚，遂行に対する報酬，報酬公平度の認知に影響を与える行為
    - ✓例：技術の重要性を説明する、遂行のレベルをほめる
- 状態遷移
  - 状態遷移は非決定性 (**確率的に遷移**)
- シナリオ
  - 初期状態S_0から最終状態S_nに至る状態の時系列
    - ✓定着成功シナリオ：技術や手法の導入成功に至るシナリオ
    - ✓定着失敗シナリオ：技術や手法の導入失敗に至るシナリオ

一意に決まらない!
どう考える?

質的研究アプローチ(コロナ前の取組み)

リサーチクエスチョン

- コースの進行中どのように受講者の動機づけが変遷するのか

フィールドデータの収集

- 受講経験者に「受講のきっかけと，受講時の状況，完了の見通し」について半構造化インタビュー(２組、計６人)

データに対するコーディング

- プロセスやその変化に着目：開発プロセス体験，時間的コスト，チームプロセスによる開眼，教員による指導の差，など.

カテゴリの分析

- 高レベルのカテゴリ：想定済みの肯定事項，想定済みの否定事項，追加的な肯定事項，追加的な否定事項

Step2 →気づいてなかった指導の問題

例：課題評価や再提出に関する指導の一部に不公平感

CAST(事故から学ぶ, 再発防止)

事故から最大限の学びを得るための基本原理を提供

- 根本原因があると思うと制御できるという幻想が生まれる
- 原因の過度の単純化（今回だと「やる気がない!」?）
- 基本的に安全コントロールストラクチャ全体に欠陥がある

事故がなぜ発生したか，を完全に理解するために「答えるべき疑問」を識別するために使うことができる.

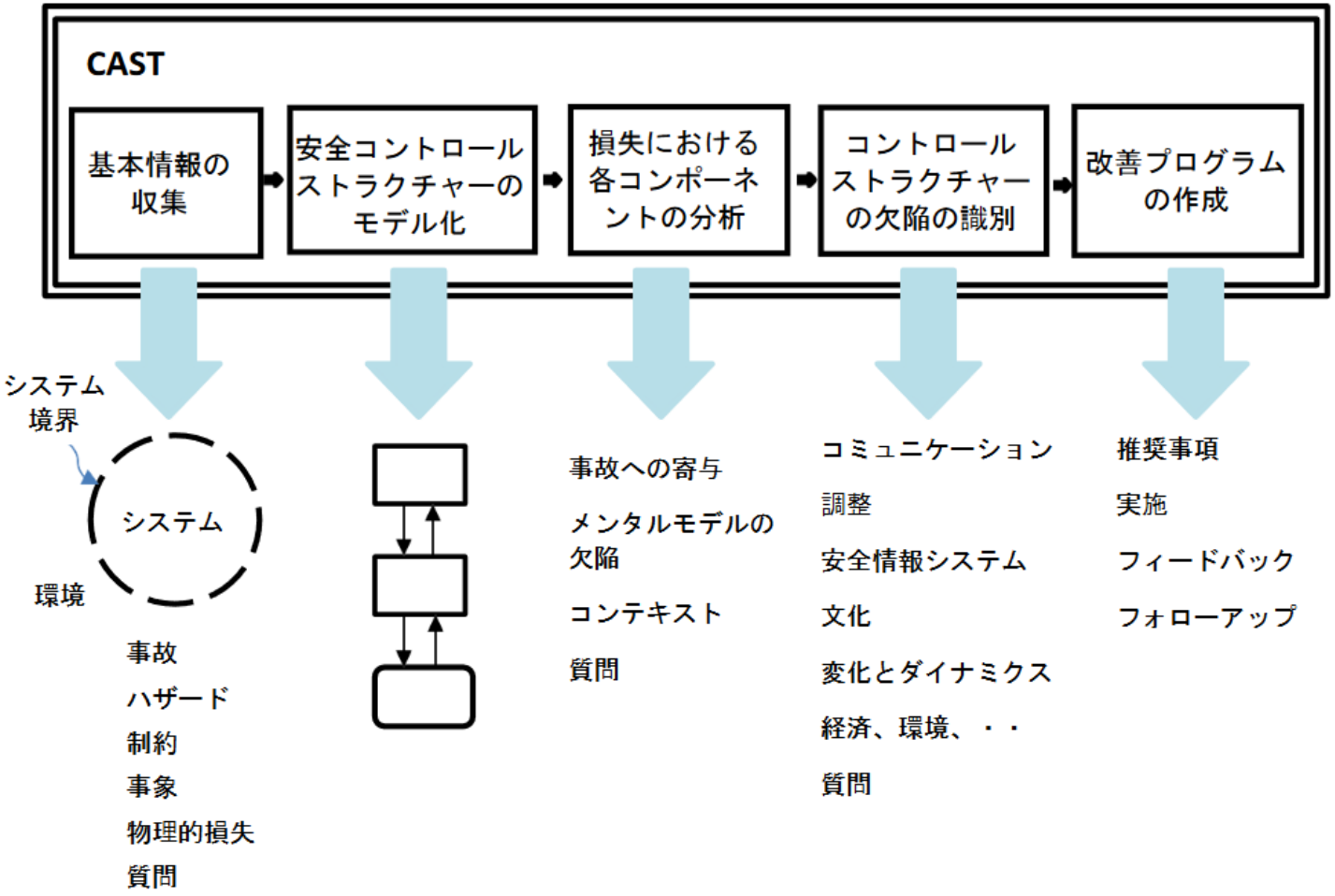
→「失敗」の使用を排除で事故から学ぶことを大きく促進

（個人的理解）

- マインドセット：ありがちな「根本原因」でとめない
- モデリングのフレームワーク：上記をサポートし再発防止を促進

CAST　分析手順

CASTハンドブックより



CAST分析1/2

1.分析を実行するための基本的な情報の収集：

a. 関連するシステムと分析の境界を定義する.
b. 損失と損失につながった危険な状態を説明する.
c. ハザードから，ハザードを防止するために必要なシステムレベルの安全制約（システムの安全要求および制約）を識別する.
d. 結論付けたり非難することなく，何が起こったのか（事象）を説明する．事象が発生した理由を説明するために回答する必要がある質問を生成する.
e. 物理的な機器とコントロールに関する物理的な喪失，関連するハザードを防止するための物理的な設計要求，この種の事故を防止するために設計に含まれる物理的なコントロール（緊急および安全のための装置），故障とハザードを引き起こす非安全な相互作用，事故を防ぐはずだった物理的なコントロールの欠落または不適切さ，および，事象に影響を与えるあらゆるコンテキスト要因，について分析する.

残りの分析の目的は，損失を許した安全コントロールストラクチャーの限界と将来それをどのように強化するかを特定すること.

CAST分析2/2

1. （前述）分析を実行するための基本的な情報の収集：
   残りの分析の目的は，損失を許した安全コントロールストラクチャーの限界と将来それをどのように強化するかを特定すること.
2. この種のハザードに対する既存の安全コントロールストラクチャーをモデル化する.
3. コントロールストラクチャーのコンポーネントを調べ，それらが損失の防止に効果的ではなかった理由を判断する：コントロールストラクチャーの下部から開始し，各コンポーネントが事故で果たした役割とその振る舞いの説明を示す（何をしたのか，なぜそのようにしたのか，また，なぜその振る舞いがその時にすべき正しいことだと思ったのか）.
4. 損失に寄与したコントロールストラクチャー全体の欠陥（一般的な体系的要因）を特定する．体系的要因は個々のシステムコントロールストラクチャーのコンポーネントにまたがる.
5. 将来同様の損失が発生するのを防ぐために，コントロールストラクチャーの変更に関する推奨事項を作成する．可能なら，全体的なリスク管理プログラムの一環として，このハザードに対する継続的改善プログラムを設計する.

おわりに

PSPトレーニングコース完了率を向上させたい

- 動機づけに着目
- 指導対象学生を動機づけモデルで表現
- 指導(動機づけの制御法)をSTAMP/STPAで分析
- 動機づけ遷移の詳細を質的アプローチで(インタビュー)+α
- 失敗事例からより多く学ぶためにCAST

指導の継続的改善

⇒トップダウンに分析・再構築(STAMP/STPA)

　動機づけ要因もトップダウン、階層的に優先順位づけ

⇒実際の失敗の効果的な分析も行う(CAST)

　失敗はボトムアップに関連要因をさかのぼる

今後：チームレベルやそれ以外にも