

本演習教材（中級編）について

独立行政法人情報処理推進機構（IPA）

デジタル基盤センター

1. 本演習教材の位置づけ.....	1
2. 演習で用いるツール（STAMP Workbench）.....	1
3. 本演習教材の概要.....	1
4. 本フォルダーに含まれるファイル.....	2
5. 演習の目的と受講対象者.....	2
6. 題材の概要.....	2
7. 演習によって得られる効果.....	3
8. 本教材の特徴.....	3
9. 演習の進め方と注意点.....	3

1. 本演習教材の位置づけ

本演習教材は、「システム思考による安全分析」の体験ができるように構成されている。すなわち、システム全体の制御構造を俯瞰する CS 図で共通認識を持ち、分析チームのメンバーが持つ様々な背景知識や想像力と、強制発想法に基づく議論によって幅広くハザードシナリオを識別する流れを、体験的に理解できることを目的としている。また、STAMP/STPA 分析を支援するツール STAMP Workbench を用いた演習であり、演習によって STAMP Workbench の基本操作を感覚的に理解することができる。

2. 演習で用いるツール（STAMP Workbench）

STAMP Workbench は、IPA からオープンソースソフトウェアとして公開しているツールである。STAMP/STPA の手順を誘導する仕組みを備えているため初心者でも迷わず分析を進められる点や、分析の各ステップで必要となる図や表が連動しているため、ステップ間の転記ミスや修正漏れを防ぎ、手間を省力化できる点が特徴である。

3. 本演習教材の概要

中級編		
	受講対象	STAMP 実適用を検討する技術者
	演習の狙い	具体的なシステムへの適用例を用いて分析の勘所を修得
	所要時間	120～150 分

所要時間にはおおよその時間を記した。演習実施の目的や受講者のレベル、受講者の人数、講師補助の人数などに応じて、時間をかけてグループ演習に重きをおく、逆に受講者のスキルに応じて解説を簡略

化する、など上記所要時間に拘らずに活用して欲しい。また、教材内容に自組織の開発対象ドメインの話題を含める／置き換えるなどのカスタマイズを行っても良い。

4. 本フォルダーに含まれるファイル

- 本演習教材（中級編）について.pdf : 本紙
- STPA 手順補足解説.pptx : STPA 手順解説における表現の違いについて補足解説
- 演習教材（中級編）.pptx : 演習で使うテキスト
- 中級-#1.stmp ~ 中級-#7.stmp : 演習の中間状態の STAMP Workbench のプロジェクトファイル
(使い方は「演習の進め方と注意点」参照)
- ライセンスについて.pdf : 本演習教材の利用許諾（ライセンス）条件 CCL-BY の説明
- ハンズオンの手引き.pdf : ハンズオン開催の準備、当日運営についての参考情報

5. 演習の目的と受講対象者

STAMP 分析の手順を概要レベルでは理解しているが、実際の分析経験が少ない人を対象として、実践的な題材の分析を通じて、STAMP の本質（システム思考のアプローチとその狙い）の理解と、真に有効な分析実施ができるようになることを目的とする。

6. 題材の概要

施設等の自動車の入退場において、入場許可のある自動車のみを入場させるための「アクセス・コントロール・ゲート」の制御システムを題材とする。下図に示すように、自動車の通行を物理的にブロックする「ゲート」とその開閉を制御する「ゲートコントローラ」があり、ゲートコントローラは、自動車を検知するセンサーと、入場許可がある場合に押される「承認ボタン」の情報をもとにゲートを開閉するシステムである。



分析対象とするシステムの概要

7. 演習によって得られる効果

分析のステップごとに課題が設定されており、グループで課題について議論しながら分析を進める形式を想定している。多様な知識を持つ分析者が CS 図によって認識を共有し、その上で意見を出し合うことにより幅広いハザード要因を得るという STAMP 分析の効果を体験できる。

また、STAMP Workbench の操作方法について、マニュアルを参照しての理解ではなく、実際に分析を行う流れにそって理解を深めることができる。

8. 本教材の特徴

自動車の入退場ゲートという比較的多くの人が想像しやすいシステムを題材としている。システムの構成要素も、車両検知センサーや昇降装置など、常識的に理解しやすいものに限定しており、題材理解の難しさが演習の妨げにならないように工夫している。

また、入場と退場が非同期に起こり、その相互干渉が起こり得る設定にしている。これにより、シンプルなシステムでありながら考えるべき状況空間が比較的広くなるため、UCA の識別やその要因分析の際に、CS 図で全体俯瞰し、幅広く相互作用を考えるというシステム思考の特徴を体験しやすいことを意図している。

演習を進める上での工夫としては、STPA の各ステップの演習を行う前にそのステップの意味を説明するページがあり、参加者はそのステップの目的を明確にしながら分析を進められるようにしている。

9. 演習の進め方と注意点

本教材は、グループディスカッションの時間を含め、2 時間から 2 時間半程度で実施することを想定している。演習の流れは以下の通りである。

- 例題の説明
- STPA Step-0 – 準備 1 (アクシデント、ハザード、安全制約の識別)
- STPA Step-0 – 準備 2 (CS 図の作成)
- STPA Step-1 (UCA の識別)
- STPA Step-2 (UCA の発生要因の分析)

STPA の各ステップは、次のような進め方を想定している。

- その分析ステップの目的や、必要となる概念等の説明
- 課題の説明
- グループ演習 (グループでのディスカッション)
- グループ演習の結果の紹介とそれに対するコメント (Q&A)
- 回答例の説明
- STAMP Workbench への入力方法の説明
- STAMP Workbench への入力の実習

演習を進める上での注意点としては、以下のような点がある。

グループ演習の結果を紹介してもらうことによって、受講者が誤解している点が明らかになることが多いため、なるべく分析の各ステップで多くのグループから結果を紹介してもらい、それをもとに質疑、解説を行うとより深い理解を導くことができる。

また、ツールの入力操作には時間がかかる場合が多いため、あらかじめ用意したプロジェクトファイルを利用するとよい。本教材では、各ステップについて、そのステップを終了した状態の **STAMP Workbench** のプロジェクトファイルが用意されている。教材資料のなかで、プロジェクトファイルが用意されているページにファイル名が書かれている。入力作業が時間内に完了できない受講者に対しては、予め配布したプロジェクトファイルを読み込むことによって、次のステップに進むように促すとよい。