

# 本演習教材（初級編）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 .....	2
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 .....	3
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 .....	4
10. 教材内容の説明 .....	4

## 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

初級編		
	受講対象	STAMP 初心者の技術者
	演習の狙い	STPA 手順概要とツール基本操作の修得
	所要時間	90 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（初級編）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（初級編）.pptx : 演習で使うテキスト
- 要求仕様.docx : 分析対象の要求仕様
- \*.stmp : 演習の各ステップに相当する STAMP Workbench のプロジェクトファイル
- 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

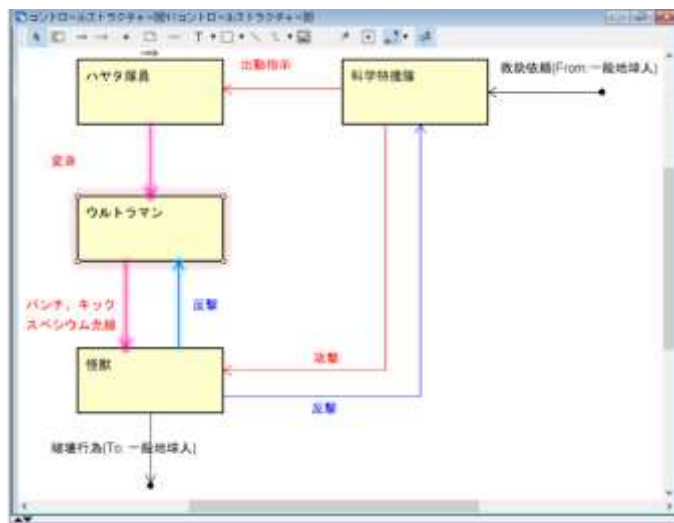
### 5. 演習の目的と受講対象者

FTA,FMEA,HAZOP など他手法による安全分析に関する知識、経験の有無に関わらず、STAMP 分析（STAMP/STPA）にはじめて取り組もうとする初心者の方、あるいは、座学で STAMP についての知識はあるが、実際に自分が手を動かして STAMP 分析をした経験のない方を対象とする。システムの相互作用に着目した STAMP 分析の手順概要を、実際に自分の手を動かして体験することにより理解してもらうことを目的とする。併せて、STAMP 分析を実施する際、効率的に分析作業を実施するために有効なツールである STAMP Workbench の基本的な操作方法を習得してもらうことも目的とする。

## 6. 題材の概要

宇宙の遠い星から地球に来たウルトラマンが、地球の科学特捜隊に協力して、地球の平和を守るために、人類を脅かす怪獣や宇宙人と戦う、という設定が本教材の題材である。

安全分析における分析対象範囲・分析対象システムは、分析の目的やステークホルダーとの合意によって決まるものである。システム俯瞰と言っても、その対象システムとはどこまでなのか、システム境界はどこなのかが重要であり、本題材はそれを考える際のヒントを与えている。本演習の Step-0 では、まず分析の目的を明確にして、CS 図を描きながら分析範囲（分析対象システムのシステム境界）を明確化している。敢えてシステム境界が自明でない題材を用いて、システム境界を決めていく過程を体験してもらう。



システムの安全構造を表す CS 図

## 7. 演習によって得られる効果

座学で得た知識を、演習で得た自分自身の経験と結びつけ、実践的なスキルへと昇華することができる。

また、STAMP Workbench が STAMP/STPA の手順を誘導するようになっていて、目的に合ったツール活用の有用性を理解できる。

## 8. 本教材の特徴

STAMP 分析の具体的な手順を理解するとともに、分析を効率的に行うために有効なツール操作に慣れることができる。

本演習では、STAMP の本質を理解するところまでは狙っていないが、短時間の演習で分析手順を正しく理解することができる。STAMP の本質を理解して、真に有効な分析を目指すには、本演習を実施した後、別途中級者向け演習を実施することを推奨する。

本演習の題材は、STAMP 分析の手順の理解に専念できる題材を選んだ。本演習の題材を既存手法で分析しようとしたら、どうやってやるか戸惑うことであろう。一方、STAMP では自然に分析ができることから、システムを俯瞰し、システムにおける相互作用に着目して分析を行う STAMP の特徴を感じるこ

とができる。

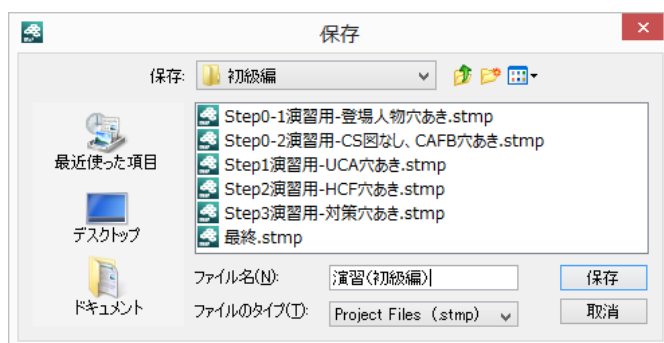
STAMP は“強制発想手法”とも言われ、分析を進める過程で新たな気づきを得られる機会が多い。本演習では、分析途中で新たな気づきを得て、前のステップに立ち戻り、分析結果の質を高めていくプロセスも経験できる。

## 9. 演習の進め方と注意点

本教材は、短時間で演習を実施できるようにしている。受講者が分析の経緯や結果の全てを入力していたのでは、分析例にならってツールに入力するだけで多くの時間がかかってしまい、受講者に考える時間を与えられなくなってしまうかねない。そこで、本教材では、各 Step で考える対象を絞り込み、入力時間よりも考える時間を多く与えられるように工夫した。具体的には、各 Step までの分析例を入力済みのプロジェクトファイルを用意している。それらのプロジェクトファイルは対象 Step までの全てを入力しているのではなく、部分的に未入力としている。受講者は、その未入力部分に絞り込んで実際の分析を行うことになる。

各 Step までの入力済みプロジェクトファイルを用いると、受講者全員が常に同じ進行状態で次の Step の演習を実施できる、というメリットがある。そして、講師にとっても全受講者に共通の解説を行えば良いというメリットがある。

下図は、プロジェクトファイルの一覧である。演習の各 Step に入るところで、対応するプロジェクトファイルを受講者全員に読み込んでもらう、という進め方を推奨する。



プロジェクトファイル一覧

本教材は短時間で実施できるように Step 毎の上記プロジェクトファイルを用意したが、時間をかけてでも一通り全部分析を経験してもらう方針であれば、利用するプロジェクトファイルを減らすなどしても良いし、プロジェクトファイル内の穴あき箇所を増やしても良い。

## 10. 教材内容の説明

ツールの誘導に沿った安全分析の手順や、効率的な分析方法を体験する。併せて、ツールの基本的な操作方法を解説している。

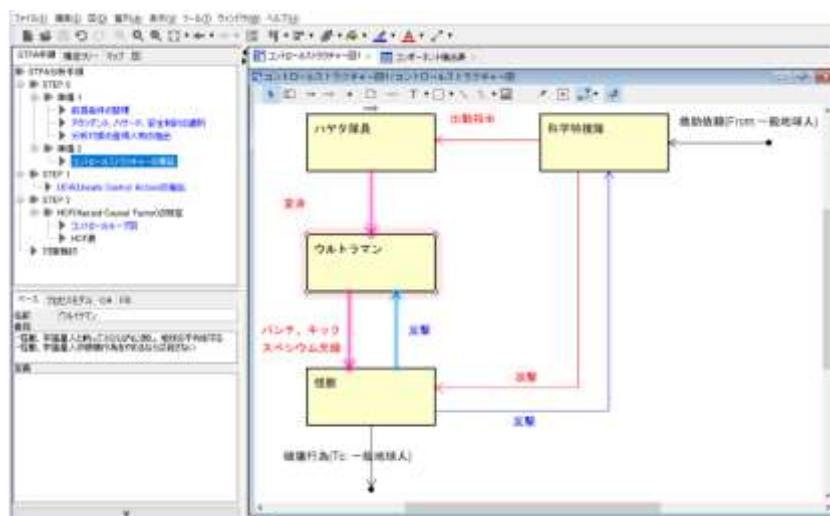
- (1) 本演習では STAMP Workbench を用いるので、ツールのインストールから受講者各自に実施してもらう。

- (2) 自然言語で記述した簡単な題材説明資料を提示して、そこに書かれた文言から要求仕様を抽出する。
- (3) グループ演習ならば、アクシデント、ハザードを何にするかをグループメンバーで議論し、合意して決める。
- (4) 要求仕様を、表を使って整理する。

コンポーネント抽出表 / コンポーネント抽出表		
同期中のCS図名：		
対象	登場人物	責務
<input checked="" type="checkbox"/>	ウルトラマン	・怪獣、宇宙星人と戦って3分以内に倒し、地球の平和を守る
<input checked="" type="checkbox"/>	怪獣	
<input checked="" type="checkbox"/>	地球征服を狙う宇宙星人	地球を征服して、地球を移住先にする
<input checked="" type="checkbox"/>	ハヤタ隊員	ウルトラマンに変身して、地球の平和を守る
<input checked="" type="checkbox"/>	一般地球人	地球で平和に暮らす

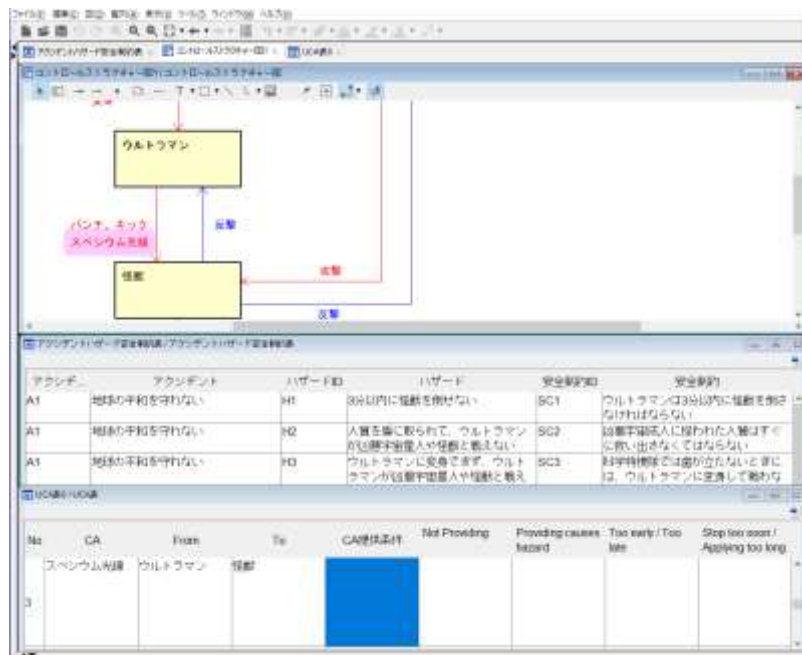
コンポーネント抽出表

- (5) STAMP Workbench の CS 図ひな型自動生成機能を用いることにより、STAMP 分析がはじめてで、CS 図とはどういうものかまったく見当がつかない受講者も分析目的と CS 図の関係を何となく理解する。
- (6) CS 図の編集をしながら、分析対象のシステム境界を明確にしていく。安全制約とコントロールアクションの関係を意識しながら CA、FB を追加・変更するプロセスを経験することにより、対象システムの安全を維持する（安全制約を守る）ための安全制御構造（コントロールストラクチャー）はどのようなものかが理解できるようになる。



CS 図編集画面

- (7) UCA を抽出する Step1 では、前提条件を与えなければ非安全になるか否かを判断できないことから、要求仕様に前提条件が不足していることに気付くようになっていく。更に、Step0 で導出した安全制約も足りないことに気付き、Step0 に立ち戻って分析を進める必要を経験する。この際、ツール支援の効果を体験できる。
- (8) Step1、Step2 に進むと、それまでに入力したいいくつかのデータを参照しながら考えることになり、ここでもツール支援の効果を体験することになる。



複数 Window を並べて表示 & プロジェクトビューを隠す表示例

- (9) 最終 Step では、STAMP/STPA の手順の範囲外ではあるが、安全分析する場合には必須となる対策検討を行い、新たな安全要求を導き出すところまでを行う。講師には、ツールを活用することによって、新たに導き出された安全要求とその背景とのトレーサビリティが確保されることを解説して欲しい。開発において、要求とその背景の関連を明確化することの重要性は解説するまでもないと思うが、必要であれば一助になることを期待する。