IPA Better Life with IT

IPA発
STAMPtool
2018.03公開予定

IPAが提供するSTAMP支援ツール i-STAMP（開発コード）

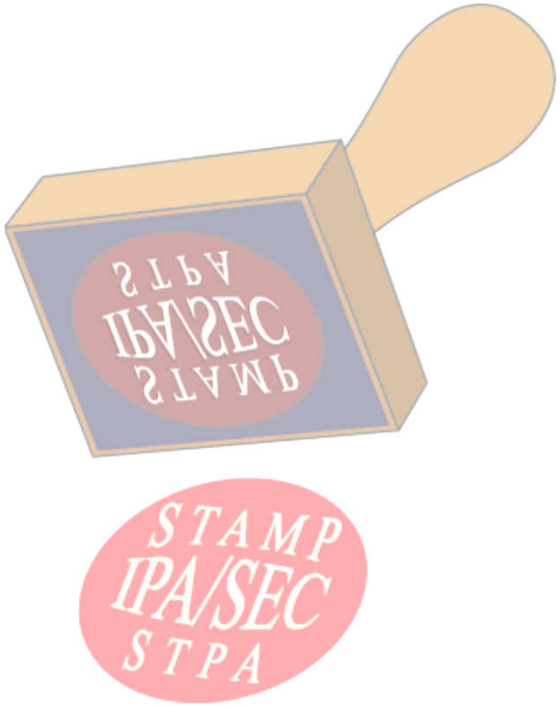
IPA/SEC will provide a STAMP based hazard analysis tool i-STAMP(code name)

独立行政法人 情報処理推進機構（IPA）
技術本部 ソフトウェア高信頼化センター（SEC）
石井 正悟
Information-technology Promotion Agency, Japan (IPA)
Software Reliability Enhancement Center (SEC)
Shogo Ishii

目 次

SEC
Software Reliability Enhancement Center

1. STAMP支援ツール開発の背景
   Background
2. STAMP普及の課題と対策
   Problems and Solutions
   1. 具体的分析手順が分からない
   2. 思考に専念できない
3. i-STAMP開発の基本コンセプト
   Basic concept of i-STAMP
4. i-STAMP概念図
   Conceptual scheme
5. i-STAMPのイメージ
   Tool image



© 2017 独立行政法人情報処理推進機構

1. STAMP支援ツール開発の背景
Background

© 2017 独立行政法人情報処理推進機構

i-STAMP開発の背景

SEC
Software Reliability Enhancement Center

- IPA/SECは2015年から安全分析技術向上手段のひとつとして、STAMPに注目して調査・研究を開始

  ⇒実システムへの適用試行により**STAMPの有効性**を確認した（実開発案件への適用は未実施）
  We confirmed the efficiency of STAMP

- 海外ではSTAMPが、これからの複雑システムの安全分析手法のデファクトスタンダードになりつつある。
  一方、我が国ではSTAMPの認知度が低い。

  ⇒海外に追いつくには、**STAMP普及展開の急加速**が必要
  Sharp acceleration to spread STAMP in Japan

2. STAMP普及の課題と対策
Problems and Solutions

© 2017 独立行政法人情報処理推進機構

STAMP普及の課題と対策

SEC
Software Reliability Enhancement Center

【課題】

- 具体的な分析手順が分からない。ガイドブックがない。

【対策】

- STAMP/STPAの具体的手順を解説するガイドを提供
  IPA developed and disclosed two kinds of STAMP/STPA guide book
  - 「はじめてのSTAMP/STPA」
  - 「はじめてのSTAMP/STPA(実践編)」

【適用時の課題と対策】

理解したつもりになるが、いざ解析しようとする と手が動かない

→ 初心者向け手順解説書を公開。各Stepで具体的に何をすべきか、どうやってInputからOutputを導き出すかの例を提示
for beginners

【実践時の課題と対策】

いざ実践してみると教科書どおりにいかない

→ 実践者向け活用方法解説書を公開。教科書で例示されているような標準的な制御構造とは異なる事例を用いて活用方法を解説
for intermediates

© 2017 独立行政法人情報処理推進機構

STAMP普及の課題と対策

SEC
Software Reliability
Enhancement Center

【課題】

- STAMP/STPAは自由な発想を引き出す強制発想手法！
  なのに思考に専念できない
  - 図表の作成・編集に手間がかかる
  - 修正に伴う影響範囲の更新に手間がかかる
- ツール活用が有効！
  しかし、分析を支援するツールがない

【対策】

- IPAがSTAMP分析支援ツールを開発し、無償公開
  - 公的機関がSTAMP支援ツールの協調領域機能を無償提供し、広範な産業分野におけるSTAMP適用を推進
  - オープンソースとしてソースコードを公開し、先行企業による適用最適化を推進

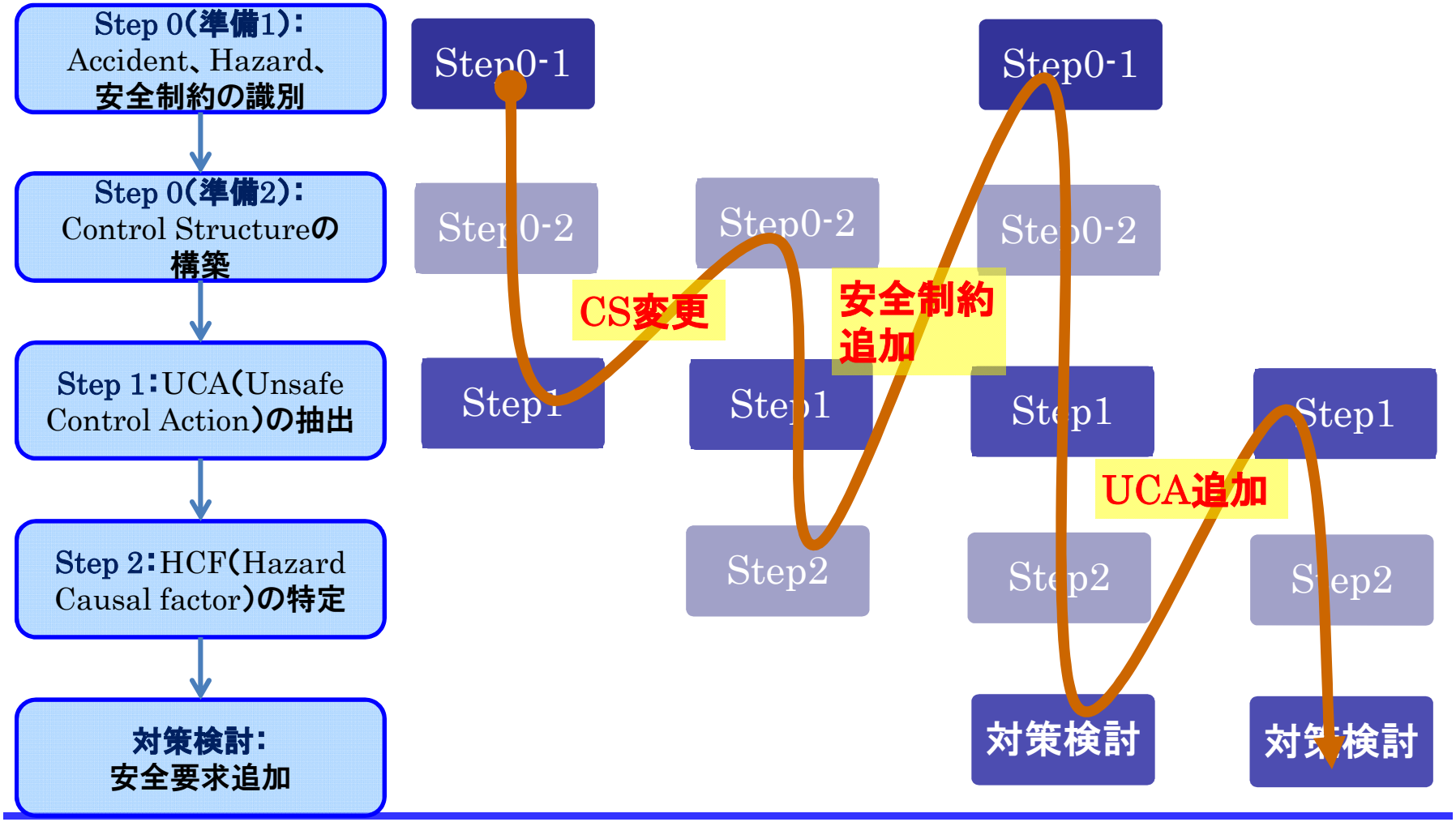
3. i-STAMP開発の基本コンセプト
Basic concept of i-STAMP

© 2017 独立行政法人情報処理推進機構

i-STAMPの基本コンセプト

SEC
Software Reliability Enhancement Center

- STPA手順を誘導し、分析者は思考に専念できる(可能な限り自動化)
- 自由な発想を引き出し、繰り返し分析を積極的に支援(リアルタイムモデル連携)
- 分析結果の妥当性を説明するためのエビデンス作成を支援



© 2017 独立行政法人情報処理推進機構

本ツールと既存ツールの違い

SEC
Software Reliability Enhancement Center

【既存のSTAMP解説書】

『Step0(準備1) ⇒ Step0(準備2) ⇒ Step1 ⇒ tStep2 』の粒度の解説であって、各Step内で実施すべき作業内容(What)や手法(How)を示していない。
繰り返し分析による網羅性向上を推奨する。

【既存ツール】

既存のSTAMP解説書の粒度の手順を実装。解説書に書かれていない各Step内の中間作業手順はブラックボックスであり、その部分にあたる分析作業を支援しない。
繰り返し分析における作業負荷低減を支援しない。

【IPAの手順解説書】

2016年4月、STAMP初心者向け手順解説書「はじめてのSTAMP/STPA」で、各Step内で実施すべきWhatとHowを具体的に示した。
2017年3月、STAMP実践者向け活用方法解説書「はじめてのSTAMP/STPA(実践編)」で、教科書通りにはいかない事例への活用方法や、ヒントを具体的に示した。

【本ツール】

IPAが提案する詳細手順(What, How, ヒント)を誘導し、分析作業を支援する。
繰り返し分析における作業負荷低減を支援する。

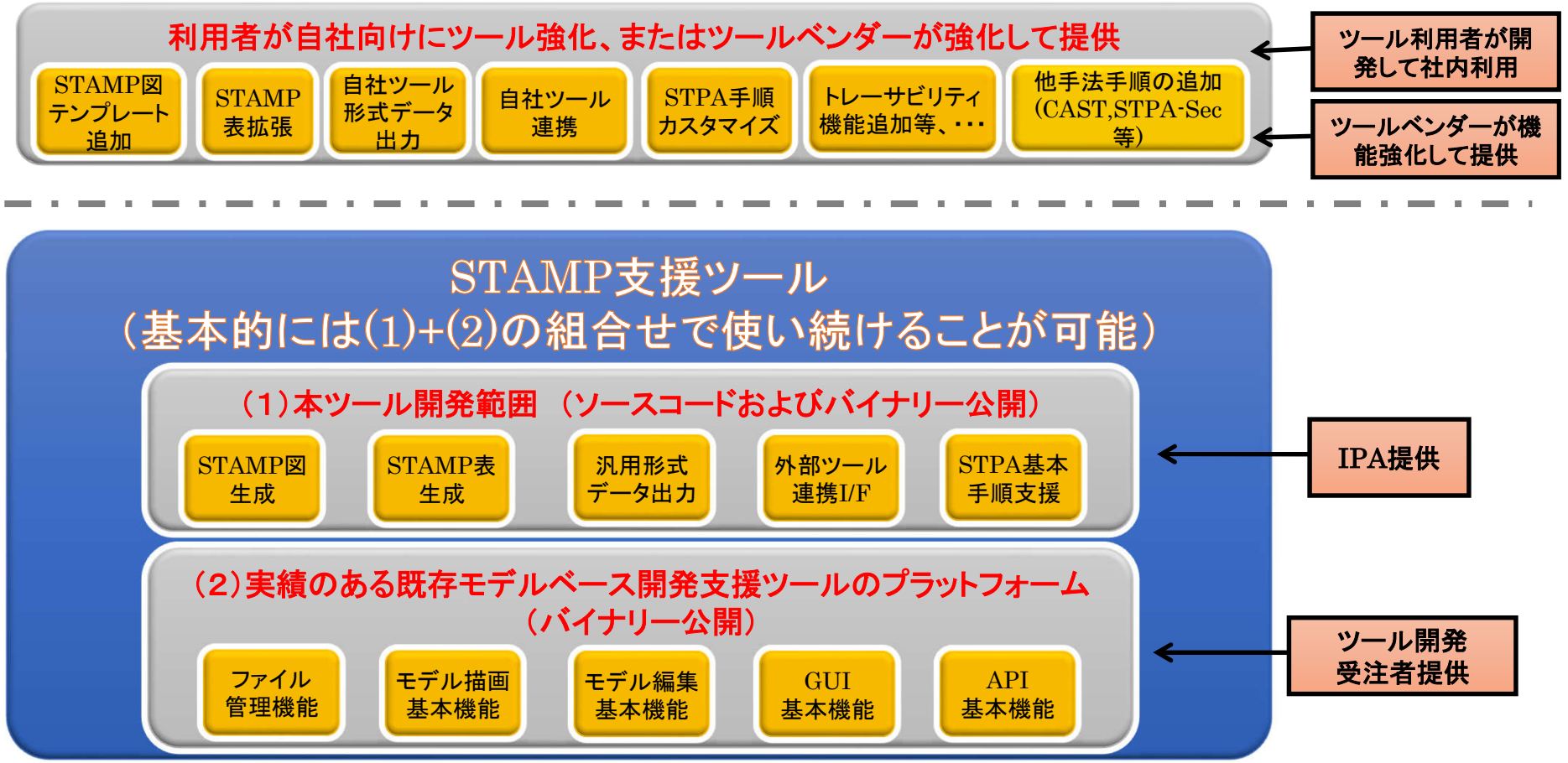
© 2017 独立行政法人情報処理推進機構

4. i-STAMPの概念図
Conceptual scheme

© 2017 独立行政法人情報処理推進機構

i-STAMPの概念図

競争領域となる拡張機能は、利用者による強化、最適化を期待する



協調領域となる基本機能を公的機関のIPAが提供し、多くの産業界での活用を推進する

© 2017 独立行政法人情報処理推進機構

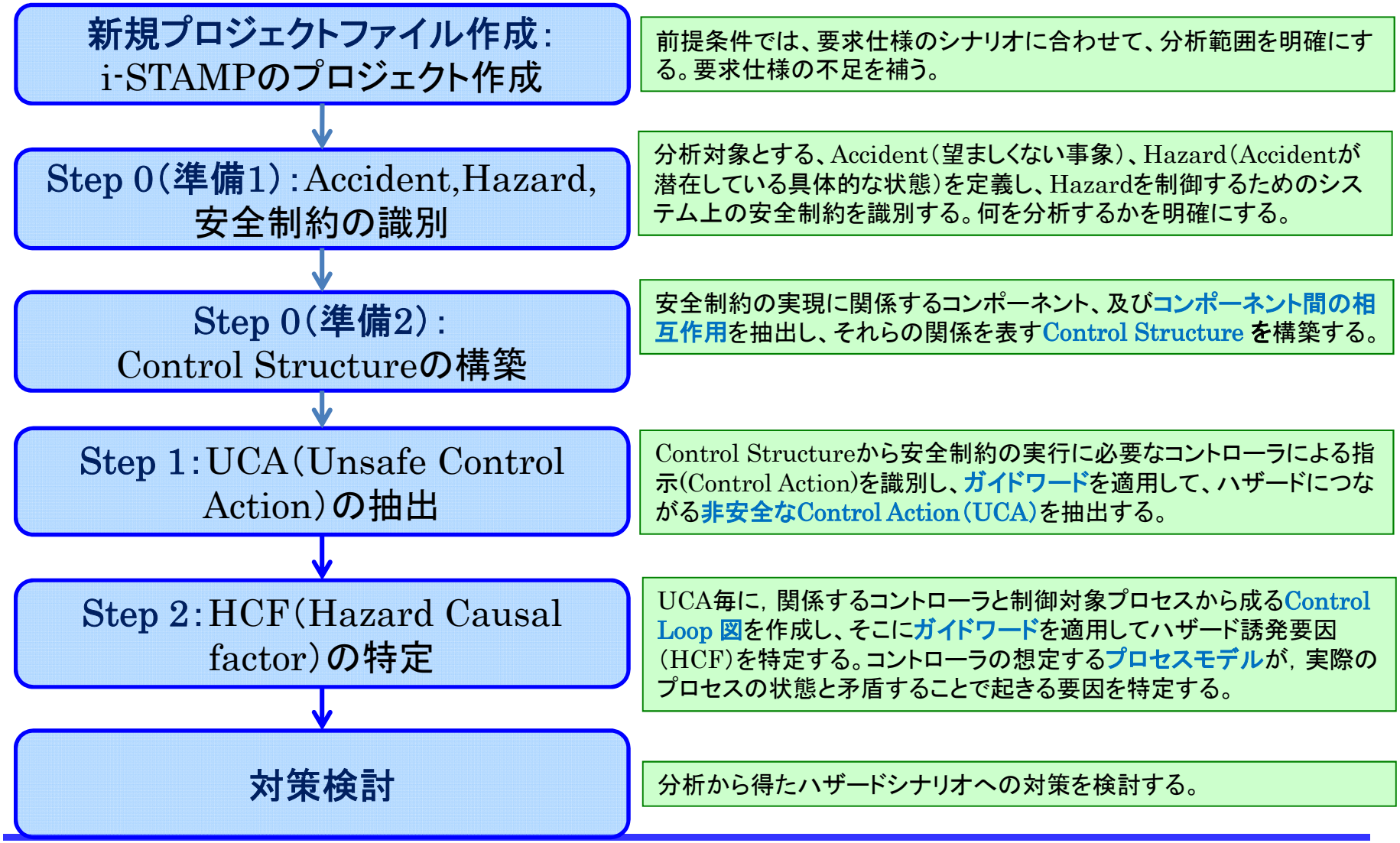
5. i-STAMPのイメージ
Tool images

© 2017 独立行政法人情報処理推進機構

STAMP/STPAの手順をツールが誘導

SEC
Software Reliability Enhancement Center

STAMP/STPA手順に沿ったi-STAMP操作手順



© 2017 独立行政法人情報処理推進機構

本ツールと既存ツールの違い(例　Step0)

SEC Software Reliability Enhancement Center

本ツールは、各Stepで作成する図や表、更に中間の過程で使用するワークシート作成の手順(IPAが推奨する手順)を誘導し、図表作成を支援する。単なるお絵描きのような作業は自動化する。
本ツールのStep0(準備2)コントロールストラクチャー構築における**分析支援機能**を示す。

既存の手順解説書やツール

Step0へのInput
自然言語で記述された仕様書

要求仕様

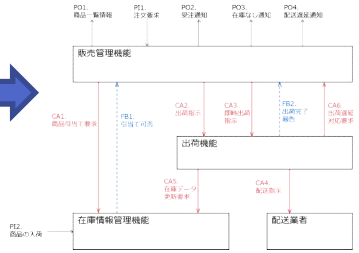
Step0(準備1)
Accident,Hazard,
安全制約の識別

Step0(準備2)
制御構造(CS)
構築

CS図を描画

手順がブラックボックスの部分を何等かの方法で考えた結果のCS図を綺麗に描画する作業を支援する(お絵描きツール)

Step0のOutput
CS図



この作業の具体的な詳細手順はブラックボックスで、ツールは分析を支援しない

本ツール

Step0へのInput
自然言語で記述された仕様書

要求仕様

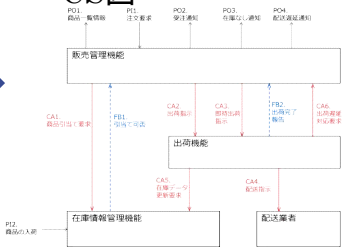
ワークシートを用いて整理

IPAが推奨する詳細手順を誘導し、分析を支援する

ワークシートから
CS図を自動生成

お絵描き作業は自動化する。
表記を自動的に統一する。IPAが推奨する表記にする

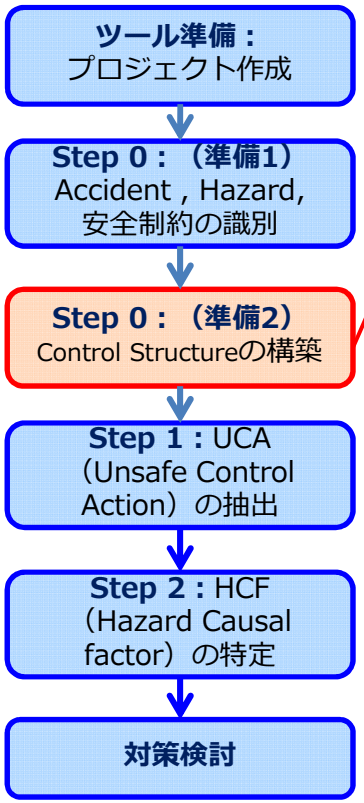
Step0のOutput
CS図



© 2017 独立行政法人情報処理推進機構

Step0 準備2：Control Structureの構築

STAMP/STPA手順に沿った
i-STAMP操作手順

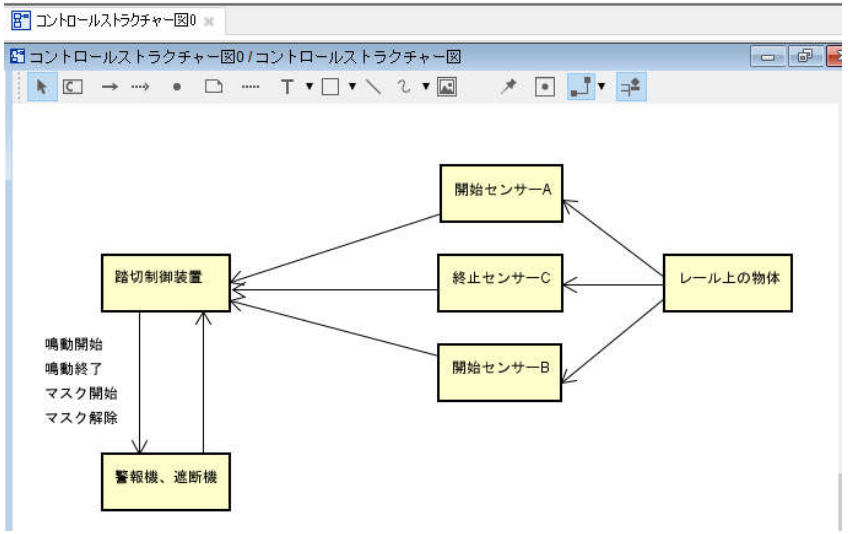


1.分析対象システムの把握
……

4.分析対象の登場人物の抽出
- 要求仕様書→コンポーネント抽出表

1.抽出した登場人物をコンポーネント
としてCS図に登場させる
- コンポーネント抽出表→CS図

コンポーネント抽出表で整理した登場人物から、分析対象のコンポーネントを選定し、安全制約の実現に関係するコンポーネント（サブシステム、機器、組織等）、及び**コンポーネント間の相互作用**（コントローラによる指示、フィードバックデータ）を抽出し、それらの関係を表す**Control Structure を**構築する。



STPAに慣れてきた技術者は、直接CS図を作図することも可能。
手順を誘導するが、ツール利用方法に制約を設けない。

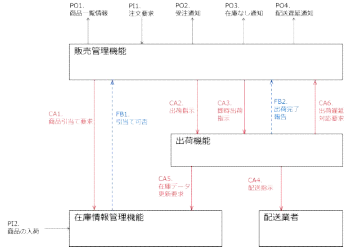
© 2017 独立行政法人情報処理推進機構

本ツールのイメージ　Step1

SEC
Software Reliability Enhancement Center

Step1へのInput
アクシデント、ハザード、安全制約一覧表、CS図、ガイドワードのセット

アクシデント(Loss)	ハザード(Hazard)	安全制約(Safety Constraints)
(A1)工事作業者・車両・機材が列車と衝突する	(H1-1)工事中に列車が踏切制御区間に進入する	(SC1-1)工事中列車を踏切制御区間に進入させてはならない
(A1)工事作業者・車両・機材が列車と衝突する	(H1-2)工事中に列車が踏切制御区間に進入した時に工事が中断(待避)されない	(SC1-2)工事中に列車進入したときは工事を中断(待避)させなければならない
(A1)工事作業者・車両・機材が列車と衝突する	(H1-3)工事中に列車が踏切制御区間に進入した時に見張り員の指示に従って停止しない	(SC1-3)工事中に列車が踏切制御区間に進入してしまった時は見張り員の指示に従わなければならない
(A2)緊急車両(消防車、救急車)が踏切を渡れず手遅れになる	(H2-1)工事中、緊急車両が来ても踏切が遮断している	(SC2-1)工事中でも緊急車両が来たら踏切を開放しなければならない
(A3)通行者・車と工事関係者・車が衝突する	(H3-1)工事中、踏切が遮断していない	(SC3-1)工事中は踏切を遮断していなければならない



Step1
Step1ではUCAを抽出する

ガイドワードは、ドメインに応じて編集、選択可能

ガイドワードのセットを編集、選択、UCA表に自動的に反映

UCA表の固定部分を自動生成

ID振り直しも自動実行

UCAにIDを自動付加
SCとのリンクを設定

UCA抽出の思考に専念してUCA表を作成

利用者は本来のUCA抽出の思考だけに専念する

Step1のOutput
UCA表

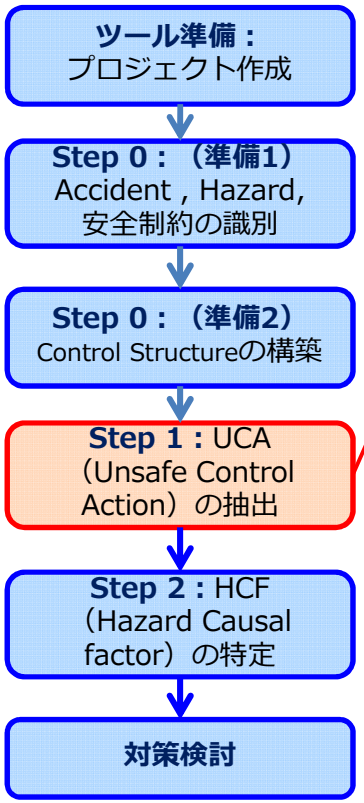
#	コントロールアクション	Not Providing	Providing causes hazard	Too early / Too late	Stop too soon / Applying too long
1	鳴動開始指示	(UCA1)警報が鳴らずに列車が踏切を通過する(踏切が閉まらない)(SC1)違反	列車が来ないのに警報が鳴る	(UCA2)警報鳴動する前に列車が踏切に到達する(閉まるのが遅(間に合わない)(SC1)違反	開始指示が継続するので、列車通過後に鳴動停止指示が出ても鳴動し続ける。
2	鳴動停止指示	列車が通過後も警報が鳴りっぱなし	(UCA3)列車が通過中に鳴動停止する(SC2)違反	(UCA3)列車が通過完了する前に鳴動停止する(閉のため後、開(のが早すぎる)(SC2)違反	(UCA1)列車通過後も鳴動停止指示が続き、次の列車が来ても鳴動しない(開始指示と競合)(SC1)違反
3	マスク開始指示	A,Cを通過した列車がBに到達した時に再鳴動する	(UCA4)列車が来ないのにマスク指示し、警報鳴動しない(UCA4)反対側の開始センサーにマスク指示し、警報鳴動しない(SC1)違反	(UCA5)終始センサーへのマスク指示が遅れ、列車の当該センサー通過に間に合わないと、マスク指示が残り、対向列車が2本続いたときに警報鳴動しない(SC1)違反	(UCA6)列車が反対側の開始センサー通過後までマスク指示し続けると、対向列車が来ても鳴動しない(SC1)違反
4	マスク解除指示	(UCA6)反対側の開始センサーにマスク解除指示が出て、対向列車が来ても鳴動しない(マスク指示後に列車が引き返す場合を含む)(SC1)違反	警報が再鳴動する	列車がBを通過完了前に出ると再鳴動する	解除を後続列車によるマスク開始指示と競合とマスクされずに再鳴動する可能性がある

© 2017 独立行政法人情報処理推進機構

Step1：UCAの抽出

SEC
Software Reliability Enhancement Center

STAMP/STPA手順に沿った
i-STAMP操作手順



1.非安全なコントロールアクションを抽出
- CS図→UCA表

Control Structureから安全制約の実行に必要なコントローラによる指示(Control Action)を識別し、**ガイドワード**を適用して、ハザードにつながる**非安全なControl Action（UCA）**を抽出する。

UCA表1 / UCA Table

No	CA	From	To	CA提供条件	Not Providing	Providing causes hazard	Too early / Too late	Stop too soon / Applying too logn
1	鳴動開始	踏切制御装置	警報機、遮断機		(UCA1-N-1) 警報が鳴らずに列車が踏切を通過する(踏切が開まらない) [SC1]	列車が来ないのに警報がなる	(UCA1-T-1) 警報鳴動する前に列車が踏切に到達する(閉まるのが遅く間に合わない)	開始指示が継続するので、列車通過後に鳴動停止指示が出ても鳴動し続ける
2	鳴動終了	踏切制御装置	警報機、遮断機		列車が通過後も警報が鳴りっぱなし	(UCA2-P-1) 列車が通過中に鳴動停止する [SC2]	(UCA2-T-1) 列車が通過完了する前に鳴動停止する(開けた後、閉くのが早すぎる) [SC2]	(UCA2-D-1) 列車通過後も鳴動停止指示が続き、次の列車が来ても鳴動しない(開始指示と競合) [SC1]
3	マスク開始	踏切制御装置	警報機、遮断機		A,Cを通過した列車がBに到達した時に再鳴動する	(UCA3-P-1) 列車が来ないのにマスク指示し、警報鳴動しない [SC1] (UCA3-P-2) 反対側の開始センサーにマスク指示し、警報鳴動しない [SC1]	(UCA3-T-1) 終止センサーへのマスク指示が遅れ、列車の当該センサー通過に間に合わないと、マスク指示が残り、対向列車が二本続いたときに警報鳴動しない [SC1]	(UCA3-D-1) 列車が反対側の開始センサー通過後までマスク指示し続けると、対向列車が来ても鳴動しない [SC1]
4	マスク解除	踏切制御装置	警報機、遮断機		(UCA4-N-1) 反対側の開始センサーにマスク解除指示が出す、対向列車が来ても鳴動しない(マスク指示後に列車が引き返す場合を含む) [SC1]	警報が再鳴動する	列車がBを通過完了前に出ると再鳴動する	解除を後続列車によるマスク開始指示と競合するとマスクされずに再鳴動する可能性がある

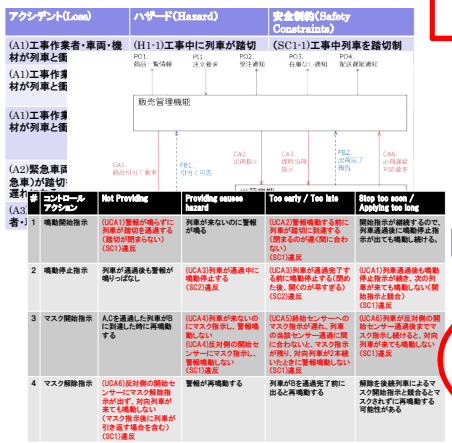
CS図を変更（例えば、CA追加/変更/削除）したら、リアルタイムで自動的にUCA表に反映。
UCAに割り当てたIDも自動的に振り直す。（振り直さないことも可。検討中）

© 2017 独立行政法人情報処理推進機構

本ツールのイメージ　Step2

SEC
Software Reliability Enhancement Center

Step2へのInput
UCA表、CS図、
ハザード・安全制約一覧表



Step2

Step2ではHCFを特定する

ヒントワードは「(人)対(機械)」等の組合せから選択

コントロールループ図を自動生成

HCF表の
固定部分を
自動生成

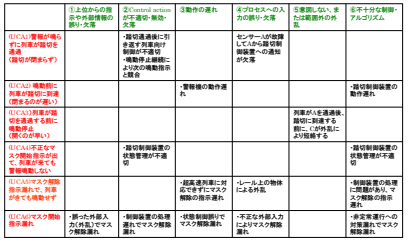
ID振り直しも自動実行

HCFにIDを自動付加
UCA、SCとのリンク
を設定

HCF特定の思考に
専念してHCF表を
作成

利用者は本来のHCF特定の思考だけに専念する

Step2のOutput
HCF表



HCF特定の作業では、いろいろな図表を参照したい。
1画面に関連図表を並べて同時に参照可能とする。
その他に参照したい図表も、リンクされた情報をクリックするだけで
容易に表示する。モデルなので、関連情報は全てリンクされている。

© 2017 独立行政法人情報処理推進機構

本ツールのイメージ　対策検討

SEC
Software Reliability Enhancement Center

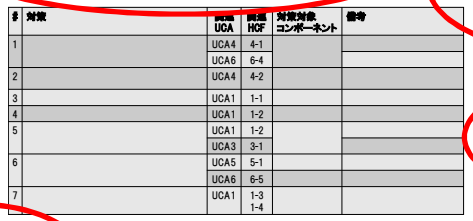
Step2へのInput
UCA表、CS図、
ハザード・安全制約一覧表

対策検討

HCFへの対策を検討・立案する

検討に必要な関連情報を即座に表示

リンクしたUCA、HCF、CS図を容易に参照



対策一覧の固定部分を自動生成

対策からの逆方向リンクも自動設定

関連HCF、UCA、SCとのリンク設定を再構築

対策立案の思考に専念する

利用者は対策立案の思考だけに専念する

Step2のOutput
HCF表

鋭意開発中

SEC
Software Reliability Enhancement Center

- 階層化CS図
  - 階層化は現時点で基本機能とは言えないかもしれないが、ニーズがあることは確か
  - いろいろなスタイルの階層化仕様が乱立することは好ましくない
  - IPAが推奨する仕様を提示することを検討中

IPA

ご清聴ありがとうございました

i-STAMPは鋭意開発中で、2018年3月にオープンソースとして無償公開予定です。

Copyright © 2017 独立行政法人情報処理推進機構

IPA