OMRON
Sensing tomorrow™

STAMPをSTAMPしてみた！

A rubber “STAMP” was analyzed using “**ST**AMP” based **P**rocess **A**nalysis.

Nov. 29, 2017

オムロンオートモーティブエレクトロニクス株式会社
OMRON Automotive Electronics Co.Ltd.
玉那覇肇
Tamanaha Hajime

発表内容

OMRON
Sensing tomorrow™

1. 背景
2. STAMPとは？
3. Step0 準備1：アクシデント，ハザード，安全制約の識別
4. Step0 準備2：コントロールストラクチャー
5. Step1：非安全なコントロールアクション(UCA)の抽出
6. Step2：HCFの特定
7. まとめ

背景

OMRON
Sensing tomorrow™

■ 2016年度に，JASPAR機能安全WG “STAMP/STPA活用ガイド開発チーム”へ参加

その成果物として，活用ガイド：
“安全性論証に使うSTAMP／STPA ～自動車編～”
を作成することになったが，その一環として，
各執筆者によるショートコラム“コーヒーブレーク”
も掲載することに．．．

そうだ！

STAMPをSTAMPしてみよう！

注意：
本日紹介する内容は，活用ガイド内の“コーヒーブレーク”と関係ありません．
活用ガイド内の“コーヒーブレーク”は，他業界への参考事例としてIPA様から発行予定書籍内に掲載される予定です．

STAMPって何？

OMRON
Sensing tomorrow™

- Systems-Theoretic Accident Model and Process：システム理論に基づくアクシデントモデルとプロセス

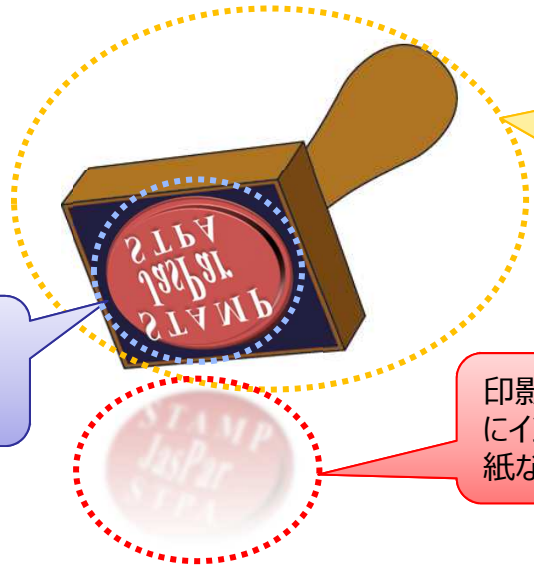
ではありません…

- ハンコ　です.

STAMPって何？

印顆（いんか）：象牙や石などに文字や絵が彫ってあり，インクや朱肉をつけて紙に押すと，文字や絵を紙にうつす事ができるもの．印章（ハンコの正式名称）やスタンプ（ゴム印）も含めた総称．

これは，あきらかにスタンプ．

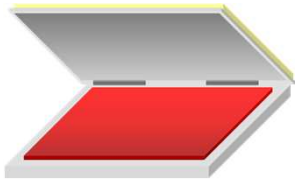


印面（いん面）：印影をとるため文字や絵が彫られている面

印影（いんえい）：印顆にインクや朱肉をつけて，紙などに押してうつしたもの

- スタンプマット：ゴム製の印押台．上から紙 ごと押し付けるように捺印して印影のカスレを防ぐ

- スタンプ台：インクをスポンジ等に浸透させ，印面を付けることでインクが付着する



STAMPでSTAMP！

OMRON
Sensing tomorrow™

【前提条件の整理】

■ 対象システム：
観光地や駅などに置かれている記念スタンプを押す

■ スタンプの押すための主要物：
- 記念スタンプ
- スタンプ台
- スタンプマット

■ スタンプを押す手順：
1. スタンプを押す紙をスタンプマットの上に置く
2. スタンプを手にとり，スタンプ台でインクを付ける
3. スタンプを押す
4. スタンプをもとの位置にもどす
5. スタンプを押した紙を取る

■ 分析手順
- 基本的に“はじめてのSTAMP/STPA（IPA2016）”に則る

発表内容

OMRON
Sensing tomorrow™

1. 背景
2. STAMPとは？
3. Step0 準備1：アクシデント，ハザード，安全制約の識別
4. Step0 準備2：コントロールストラクチャー
5. Step1：非安全なコントロールアクション(UCA)の抽出
6. Step2：HCFの特定
7. まとめ

Step0 準備1：アクシデント，ハザード，安全制約の識別

■ “**アクシデント**”を定義します！
観光地などで記念スタンプを押した時のアクシデントってなんだろう？
- 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
- 損失：人命喪失，けが，物損，環境汚染，ミッション喪失，経済的損失など

失敗したと感じた瞬間のこと．．．

- 印影に斑ができてしまった．．．
  ⇒(アクシデントA1)印影に斑ができる
- 印影が傾いてしまった．．．
  ⇒(アクシデントA2)印影が斜め/上下逆になる
- 押したかった場所から微妙にずれてしまった．．．
  ⇒(アクシデントA3)印影が押したかった場所からずれる

Step0 準備1：アクシデント，ハザード，安全制約の識別

■ 続いて，アクシデントに対する“**ハザード**”を定義します．

- ハザード：環境のある最悪な条件と重なることでアクシデントにつながるような、システムの状態もしくは条件
- ハザードは，コントロール対象のシステムの範囲内

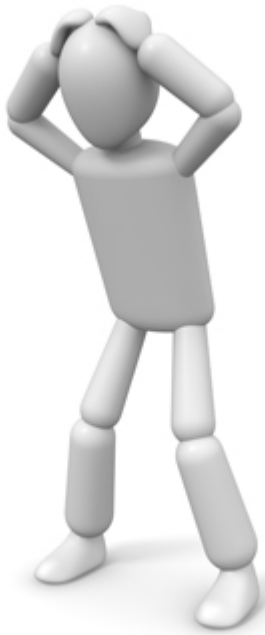
(A1)印影に斑ができる

⇒(H1-1)印面の面が平らでない

⇒(H1-2)印面にインクが均一についてない

⇒(H1-3)スタンプマットの面が平らでない

(A2・・・



■ “**安全制約**”はハザードの裏返しとなります．

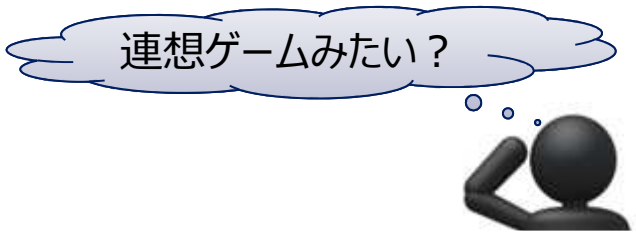
表でまとめると…

Step0 準備1：アクシデント，ハザード，安全制約の識別

OMRON
Sensing tomorrow™

■ 表　Step0　アクシデント，ハザード，安全制約の識別

アクシデント	ハザード	安全制約
(A1)印影に斑ができる	(H1-1)印面の面が平らでない	(SC1-1)印面は平らにしなければならない
	(H1-2)印面にインクが均一についてない	(SC1-2)印面にインクを均一につけなければならない
	(H1-3)スタンプマットの面が平らでない	(SC1-3)スタンプマットの面は平らにしなければならない
(A2)印影が斜め/上下逆になる	(H2-1)印章の上下方向が分かりにくい	(SC2-1)印章の上下方向を分かり易くするようにしなければならない
(A3)印影が押したかった場所からずれる	(H3-1)印影の位置が分かりにくい	(SC3-1)印影の位置を分かり易くするようにしなければならない



発表内容

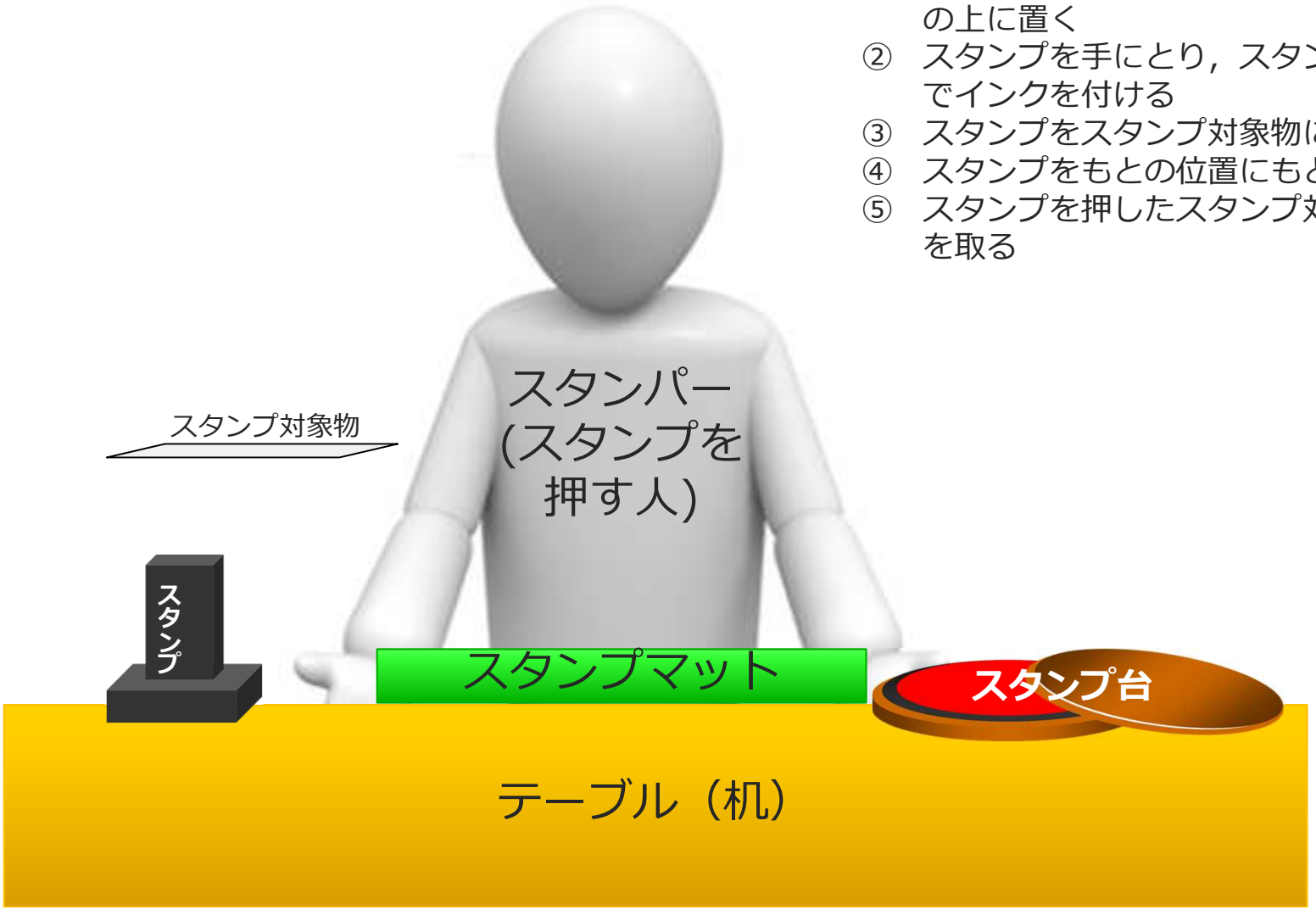
OMRON
Sensing tomorrow™

1. 背景
2. STAMPとは？
3. Step0 準備1：アクシデント，ハザード，安全制約の識別
4. Step0 準備2：コントロールストラクチャー
5. Step1：非安全なコントロールアクション(UCA)の抽出
6. Step2：HCFの特定
7. まとめ

Step0 準備2：コントロールストラクチャー

■ システム構成要素の再確認

① スタンプ対象物をスタンプマットの上に置く
② スタンプを手にとり，スタンプ台でインクを付ける
③ スタンプをスタンプ対象物に押す
④ スタンプをもとの位置にもどす
⑤ スタンプを押したスタンプ対象物を取る

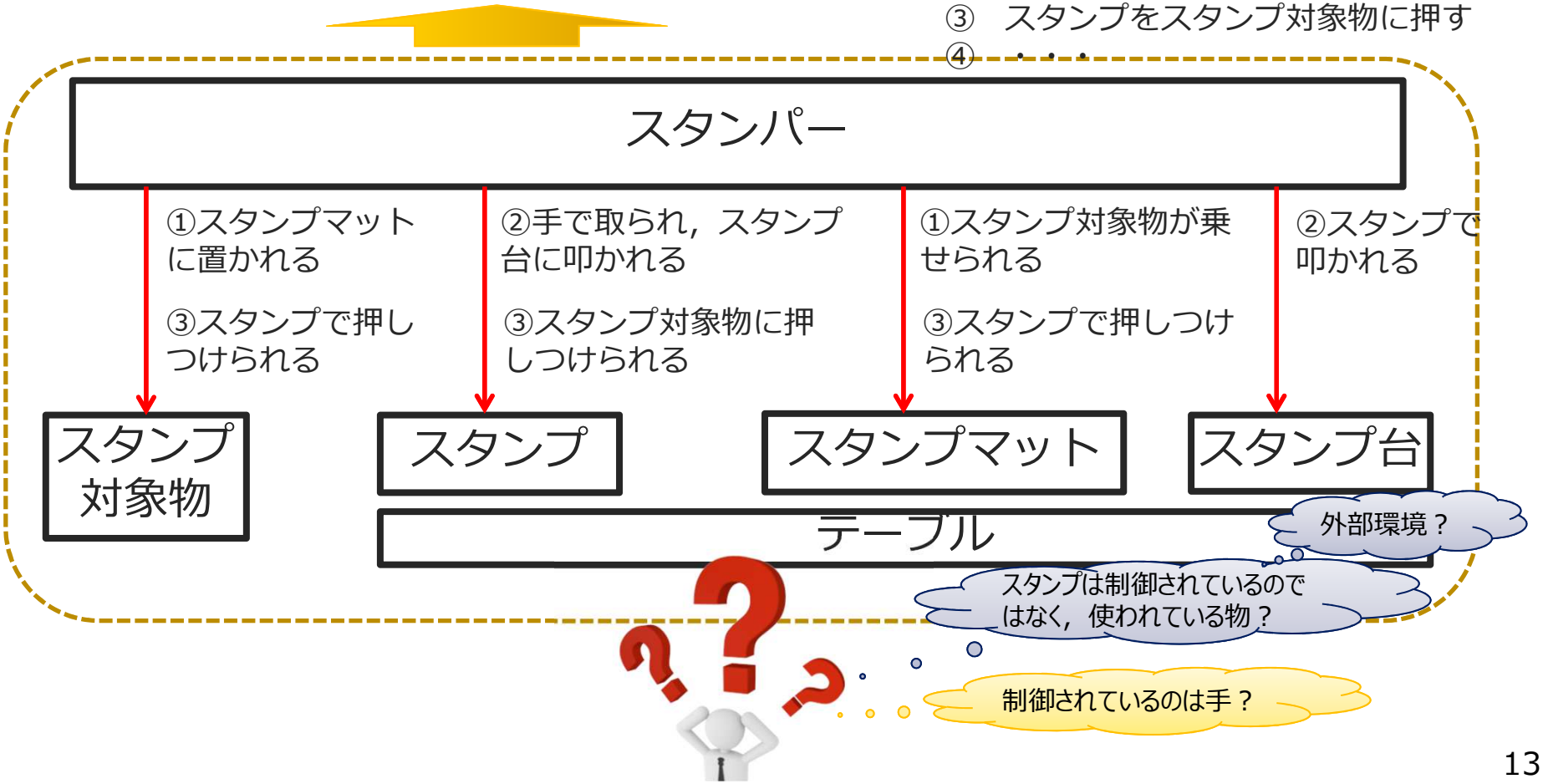


Step0 準備2：コントロールストラクチャー

■ コントロールストラクチャーを構築します．

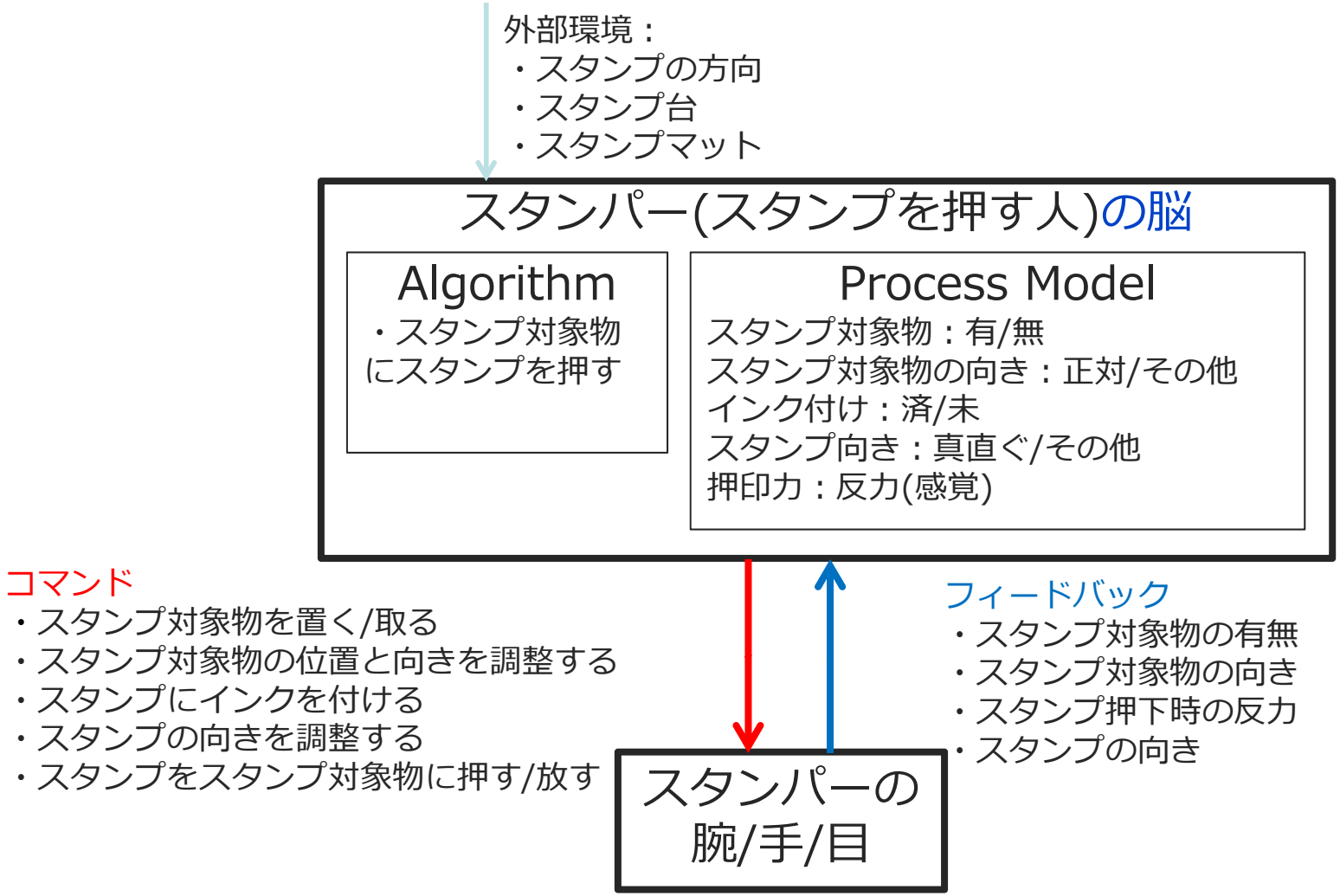
“制御している物”と“制御されている物”を明確にし，まとめられるものはまとめることで抽象度を上げる

① スタンプ対象物をスタンプマットの上に置く
② スタンプを手にとり，スタンプ台でインクを付ける
③ スタンプをスタンプ対象物に押す
④ ・・・



Step0 準備2：コントロールストラクチャー

■ コントロールストラクチャー



発表内容

OMRON
Sensing tomorrow™

1. 背景
2. STAMPとは？
3. Step0 準備1：アクシデント，ハザード，安全制約の識別
4. Step0 準備2：コントロールストラクチャー
5. Step1：非安全なコントロールアクション(UCA)の抽出
6. Step2：HCFの特定
7. まとめ

Step1：非安全なコントロールアクション(UCA)の抽出

OMRON
Sensing tomorrow™

Generalな手法はアドホックなので初心者の最大の悩み所

⇒ STPA Step1とUCA特定のための“システマチック手法”でStep1を行います

- An STPA Primer Version 1, August 2013 (updated June 2015)
  Chapter 3: Formal Tools to Support STPA

■ UCA特定のための主要素はなにか？
ポイント：コントロールアクション(CA)それ自身だけでUnsafeにならない
例えば，“スタンプをスタンプ対象物に押す”というCAは，Unsafe？
⇒答えは，場合（状況）によりけり.

**UCAを特定するには，
コンテキスト(状況)を明確にすることが必要**

コンテキストは，

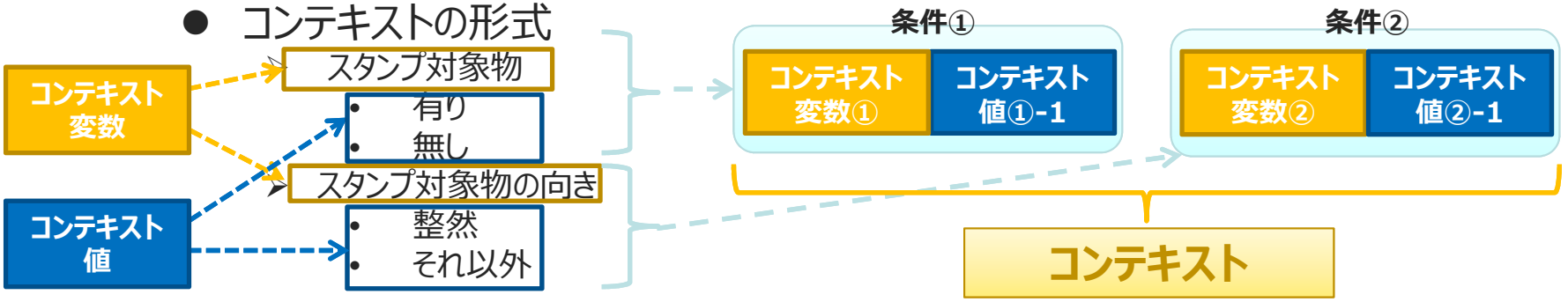
- アクションがハザードにつながる，システムと環境の状態
- プロセスモデルの肝心な部分

Step1：非安全なコントロールアクション(UCA)の抽出

OMRON
Sensing tomorrow™

■ コンテキストとは？

● コンテキストの形式



条件は１組の変数と値で表され，コンテキストは1つ以上の条件の組み合わせ

分析時は，全ての条件の組み合わせを考える

■ UCAを4つの要素で作ります（UCAの構文）

スタンパーが，スタンプ対象物が有りスタンプ対象物の向きが整然としていない時に，スタンプをスタンプ対象物に押す を行う，

ソース：コントロールアクションを与えるコントローラ

コンテキスト：Unsafeを引き起こす，システムの“状態”

コントロールアクション：実際のコマンド

タイプ：コントロールアクションを“与える”か，“与えない”かの何れか

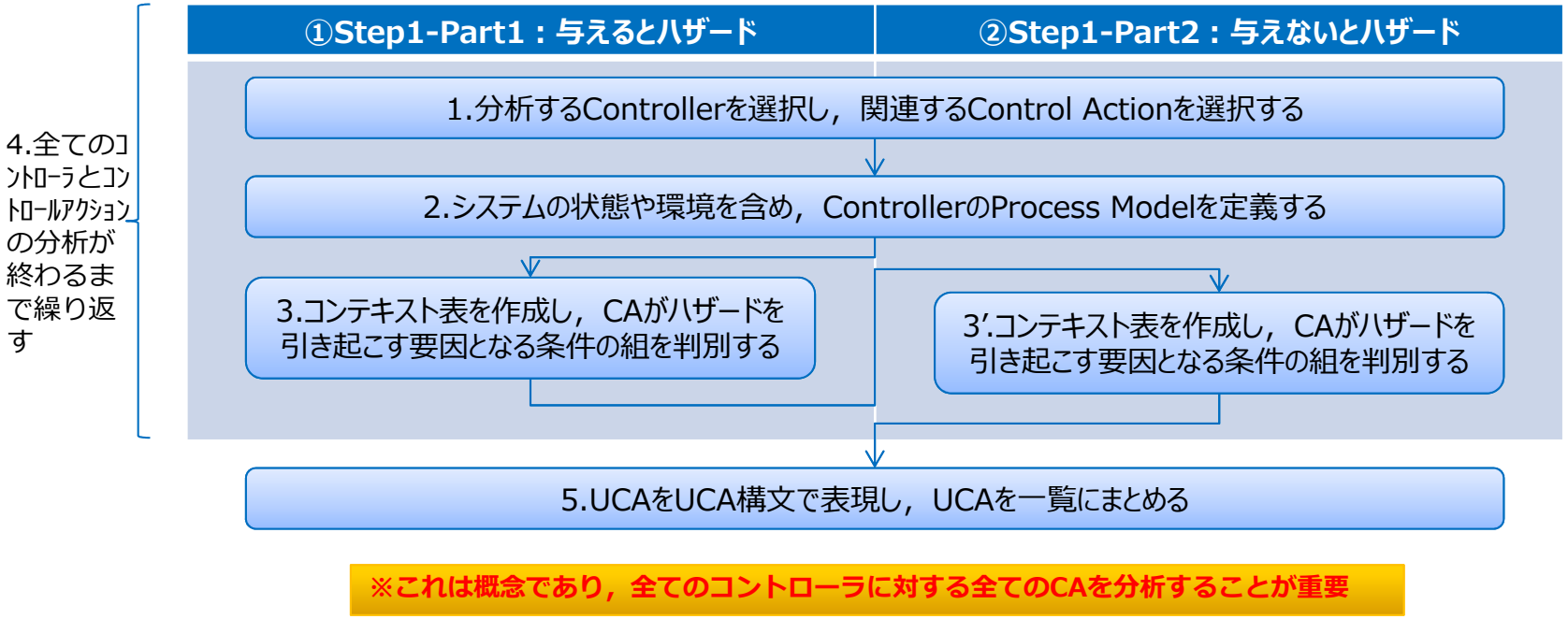
Step1：非安全なコントロールアクション(UCA)の抽出

OMRON
Sensing tomorrow™

■ “システマチック手法”の手順は？

システマチック手法は2パートで構成されており，“CAを与える”と“CAを与えない”のパートに分かれています．

1. CS図から分析するコントローラとコントロールアクションを選択する
2. コントローラのプロセスモデルと定義する
3. コンテキスト表を作成し，UCAを判定
4. コントローラとコントロールアクションの全ての組み合わせを分析します．
5. UCA構文をつかって，UCA表(4つのタイプのHCAが定義された表)にまとめます．

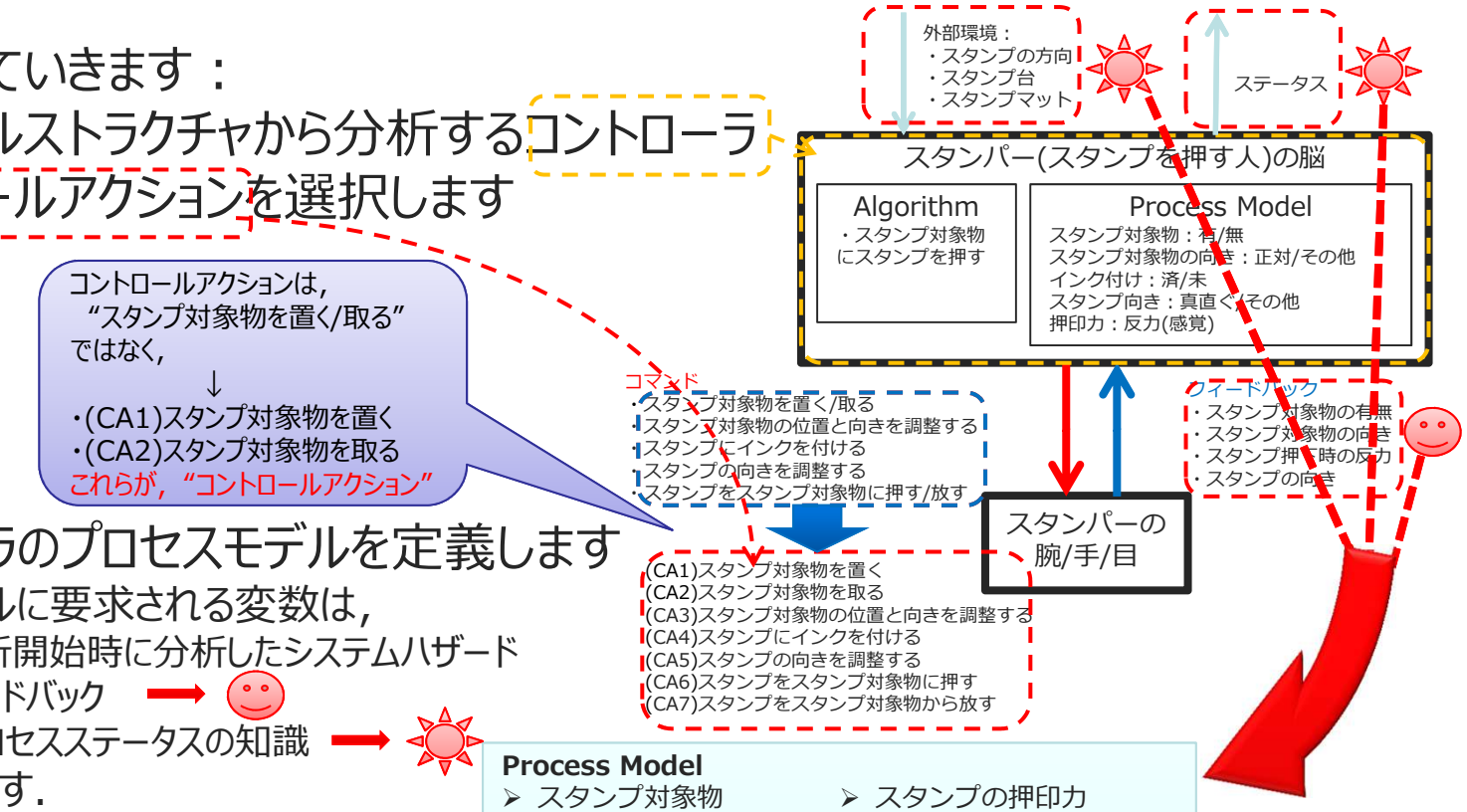


※これは概念であり，全てのコントローラに対する全てのCAを分析することが重要

Step1：非安全なコントロールアクション(UCA)の抽出

実際に分析していきます：

1. コントロールストラクチャから分析するコントローラとコントロールアクションを選択します



コントロールアクションは，
“スタンプ対象物を置く/取る”
ではなく，
↓
・(CA1)スタンプ対象物を置く
・(CA2)スタンプ対象物を取る
これらが，“コントロールアクション”

2. コントローラのプロセスモデルを定義します

プロセスモデルに要求される変数は，

- STPA分析開始時に分析したシステムハザード
- CSのフィードバック →
- 環境やプロセスステータスの知識 →

から導出します．

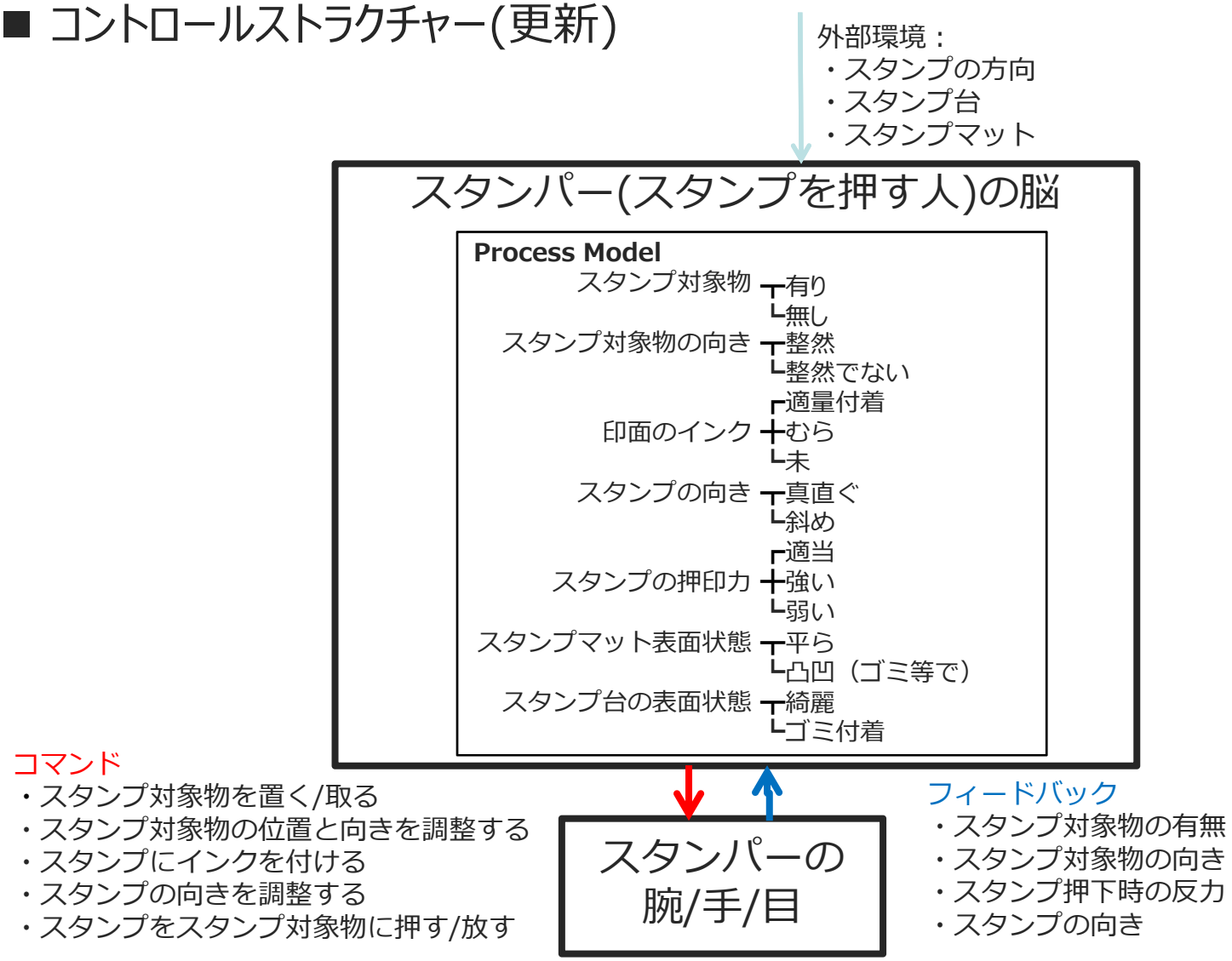
(H1-1)印面の面が平らでない
(H1-2)印面にインクが均一についてない
(H1-3)スタンプマットの面が平らでない
(H2-1)印章の上下方向が分かりにくい
(H3-1)印影の位置が分かりにくい

Process Model

- スタンプ対象物
  - 有り
  - 無し
- スタンプ対象物の向き
  - 整然
  - 整然でない
- 印面のインク
  - 適量付着
  - むら
  - 未
- スタンプの向き
  - 真直ぐ
  - 斜め
- スタンプの押印力
  - 適当
  - 強い
  - 弱い
- スタンプマット表面状態
  - 平ら
  - 凸凹（ゴミ等で）
- スタンプ台の表面状態
  - 綺麗
  - ゴミ付着

Step1：非安全なコントロールアクション(UCA)の抽出

■ コントロールストラクチャー(更新)



Step1：非安全なコントロールアクション(UCA)の抽出

OMRON
Sensing tomorrow™

3. コンテキスト表を作成し，UCAを特定します

■ コンテキスト表．“スタンプにインクを付ける”を与えるとハザード

コンテキスト変数

UCAになるか判定

#	CA	印面のインク	スタンプの押印力	スタンプ台の表面状態	UCA？ 与える	与える事が早すぎ	与える事が遅すぎ	与える事が長過ぎ	与える事が短すぎ
4	（スタンプ台で）スタンプにインクを付ける	未	適当	綺麗	H1-2	–	–	New:濃い	New:薄い
		未	適当	ゴミ付着	New:ゴミ	–	–	–	–
		未	強い	綺麗	New:濃い	–	–	–	–
		未	強い	ゴミ付着	New:濃い /ゴミ	–	–	–	–
		未	弱い	綺麗	New:薄い	–	–	–	–
		未	弱い	ゴミ付着	New:薄い /ゴミ	–	–	–	–
		むら	適当	綺麗					
		むら	適当	ゴミ付着					
		むら	強い	綺麗					
		むら	強い	ゴミ付着					
		むら	弱い	綺麗					
		むら	弱い	ゴミ付着					
		適量付着・・・	・・・	・・・					

CAのSafe/Unsafe影響がない条件：

- スタンプ対象物
- スタンプの向き
- スタンプ対象物の向き
- スタンプの押印力

関連するハザード：
•(H1-2)印面にインクが均一についてない

Step1：非安全なコントロールアクション(UCA)の抽出

OMRON
Sensing tomorrow™

■ コンテキスト表．“スタンプにインクを付ける”を与えるとハザード（更新）

#	CA	印面のインク	スタンプの押印力	スタンプ台の表面状態	UCA？				
					与える	与える事が早すぎ	与える事が遅すぎ	与える事が長過ぎ	与える事が短すぎ
4	（スタンプ台で）スタンプにインクを付ける	未	適当	綺麗	H1-2	–	–	New:濃い	New:薄い
		未	強い	(無関係)	New:濃い	–	–	–	–
		未	弱い	(無関係)	New:薄い	–	–	–	–
		未	(無関係)	ゴミ付着	New:ゴミ	–	–	–	–
		むら	(無関係)	(無関係)	New:むら	–	–	–	–
		適量付着	(無関係)	(無関係)	New:濃い	–	–	–	–

■ コンテキスト表．“スタンプにインクを付ける”を与えないとハザード

#	CA	印面のインク	UCA？
			与えない
4	（スタンプ台で）スタンプにインクを付ける	未	New:付かない
		むら	New:薄い／むら
		適量付着	– (ほぼありえない)

全てのコントローラと，全CAの分析が終わるまで繰り返します

Step1：非安全なコントロールアクション(UCA)の抽出

OMRON
Sensing tomorrow™

■ コンテキスト表（まとめ）

#	CA	スタンプ対象物	スタンプ対象物の向き	印面のインク	スタンプの向き	スタンプの押印力	スタンプマットの表面状態	スタンプ台の表面状態	UCA？					
									与えない	与える	与える事が早すぎ	与える事が遅すぎ	与える事が長過ぎ	与える事が短すぎ
1	スタンプ対象物を（スタンプマット上に）置く	無し	(無関係)	(無関係)	(無関係)	(無関係)	平らでない	(無関係)	※	H1-3	–	–	–	–
		有り	(無関係)	(無関係)	(無関係)	(無関係)	(無関係)	(無関係)	※	H1-3	–	–	–	–
2	スタンプ対象物を（スタンプマット上から）取る	(無関係)	(無関係)	(無関係)	(無関係)	(無関係)	(無関係)	(無関係)	※	※	※	※	※	※
3	（スタンプマット上の）スタンプ対象物の位置と向きを調整する	有り	整然でない	(無関係)	(無関係)	(無関係)	(無関係)	(無関係)	H2-2(★)	※	※	※	※	※
		無し	(無関係)	(無関係)	(無関係)	(無関係)	(無関係)	(無関係)	※	※	※	※	※	※
4	（スタンプ台で）スタンプにインクを付ける	(無関係)	(無関係)	未	(無関係)	(無関係)	(無関係)	(無関係)	H4-1(★)	H1-1	–	–	H5-2(★)	H4-3(★)
		(無関係)	(無関係)	未	(無関係)	適当	(無関係)	綺麗	–	H1-2 H4-2	–	–	–	–
		(無関係)	(無関係)	未	(無関係)	強い	(無関係)	(無関係)	–	H4-3(★)	–	–	–	–
		(無関係)	(無関係)	未	(無関係)	弱い	(無関係)	(無関係)	–	H5-1(★)	–	–	–	–
		(無関係)	(無関係)	未	(無関係)	(無関係)	(無関係)	ゴミ付着	–	H6-1(★)	–	–	–	–
		(無関係)	(無関係)	むら	(無関係)	(無関係)	(無関係)	(無関係)	H4-1(★)	※	※	※	※	※
		(無関係)	(無関係)	適量付着	(無関係)	(無関係)	(無関係)	(無関係)	※	※	※	※	※	※
5	（スタンプを対象物に押す前に）スタンプの向きを調整する	有り	(無関係)	(無関係)	斜め	(無関係)	(無関係)	(無関係)	※	H2-1	–	–	–	–
		無し	(無関係)	(無関係)	(無関係)	(無関係)	(無関係)	(無関係)	※	※	※	※	※	※
6	スタンプをスタンプ対象物に押す	有り	(無関係)	(無関係)	(無関係)	(無関係)	(無関係)	(無関係)	※	H3-1	–	H4-4(★)	–	–
		無し	(無関係)	(無関係)	(無関係)	(無関係)	(無関係)	(無関係)	※	※	※	※	※	※
7	スタンプをスタンプ対象物から放す	(無関係)	(無関係)	(無関係)	(無関係)	(無関係)	(無関係)	(無関係)	※	※	※	※	※	※

★印：STPA分析開始時に分析できなかったハザード

前提条件：①スタンプを押す意思がある人の行動なので，スタンプを押す基本的な行為は行う事としました
②CAを提供する際に，目で見て判断できる不備の条件は分析対象外としました

Step1：非安全なコントロールアクション(UCA)の抽出

OMRON
Sensing tomorrow™

■　つづいて，分析結果をUCA構文を用いてUCA表にまとめます

◆UCA表（1/2）

#	コントロールアクション	Not Providing	Providing causes hazard	Too early/Too late	Stop too soon/Apply too long
1	スタンプ対象物を（スタンプマット上に）置く	–	●(CA1-P1)スタンパーが，スタンプマット表面上に凹凸があるところに，スタンプ対象物を置く／SC1-3違反 ★(CA1-P2)スタンパーが，スタンプマット上に物が置かれているところに，スタンプ対象物を置く／SC1-4違反	–	–
2	スタンプ対象物を（スタンプマット上から）取る	–	–	–	–
3	（スタンプマット上の）スタンプ対象物の位置と向きを調整する	★(CA3-NP1)スタンパーが，スタンプ対象物が整然と置かれてない時に，スタンプ対象物の位置と向きを調整しない／SC2-2違反	–	–	–
4	（スタンプ台で）スタンプにインクを付ける	★(CA4-NP1) スタンパーが，スタンプにインクをつけない／SC4-1違反	●(CA4-P1)スタンパーが，印面が平らでないスタンプに，インクを付ける／SC1-1違反 ●(CA4-P2)スタンパーが，スタンプ台の表面が綺麗でスタンプの押印力が適切に，スタンプにインクを付ける(？印面に均一につかない)／SC1-2違反 ・・・	–	★(CA4-D1)スタンパーが，スタンプにインクを付ける時間が短かすぎる／SC4-3違反 ★(CA4-D2)スタンパーが，スタンプにインクを付ける時間が長すぎる／SC5-2違反

★印：STPA分析開始時に分析できなかったハザードにつながるUCA
？印：UCA構文だけではUCAと判断できないが，UCAと判断した理由

Step1：非安全なコントロールアクション(UCA)の抽出

◆UCA表（2/2）

#	コントロールアクション	Not Providing	Providing causes hazard	Too early/Too late	Stop too soon/Apply too long
4	（スタンプ台で）スタンプにインクを付ける	・・・	・・・ ★(CA4-P3)スタンパーが，スタンプ台の表面が綺麗でスタンプの押印力が適切に，スタンプにインクを付ける（？インク量不足）／SC4-2違反 ★(CA4-P4)スタンパーが，押印力を弱で，スタンプにインクを付ける／SC4-3違反 ★(CA4-P5)スタンパーが，押印力を強で，スタンプにインクを付ける／SC5-1違反 ★(CA4-P6)スタンパーが，スタンプ台にゴミ類が付着した状態で，スタンプにインクを付ける／SC6-1違反	・・・	・・・
5	（スタンプを対象物に押す前に）スタンプの向きを調整する	－	●(CA5-P1)スタンパーが，スタンプの向きが斜めの時，印面の向きを調整する（？調整量不足）／SC2-1違反	－	－
6	スタンプをスタンプ対象物に押す	－	●(CA6-P1)スタンパーが，スタンプをスタンプ対象物に押す（？印影位置不認識）／SC3-1違反 ★(CA6-P2)スタンパーが，スタンプをスタンプ対象物に押す（？印面部に均一に押印力がかからない）／SC1-5違反	★(CA6-T1)スタンパーが，スタンプをスタンプ対象物に押すのに時間がかかり過ぎる(インクが生乾き)／SC4-4違反	－
7	スタンプをスタンプ対象物から放す	－	－	－	－

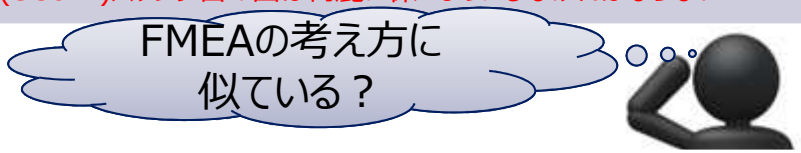
★印：STPA分析開始時に分析できなかったハザードにつながるUCA
？印：UCA構文だけではUCAと判断できないが，UCAと判断した理由
⇒プロセスモデルの不足が原因（要：イタレーション）

Step1：アクシデント，ハザード，安全制約の識別（更新）

OMRON
Sensing tomorrow™

■ 表 Step0 アクシデント，ハザード，安全制約の識別（更新）

アクシデント(Loss)	ハザード(Hazard)	安全制約(Safety Constraints)
(A1)印影に斑ができる	(H1-1)印面の面が平らでない	(SC1-1)印面は平らにしなければならない
	(H1-2)印面にインクが均一についてない	(SC1-2)印面にインクを均一につけなければならない
	(H1-3)スタンプマットの面が平らでない	(SC1-3)スタンプマットの面は平らにしなければならない
	(H1-4)スタンプマットの上に物が置かれている	(SC1-4)スタンプマット上の物を取り除かなければならない
	(H1-5)印面に均一に押印力がかからない	(SC1-5)印面に均一に押印力がかかるようにしなければならない
(A2)印影が斜め/上下逆になる	(H2-1)印章の上下方向が分かりにくい	(SC2-1)印章の上下方向を分かり易くするようにしなければならない
	(H2-2)スタンプ対象物が整然と置かれない	(SC2-2)スタンプ対象物を整然と置かれるようにしなければならない
(A3)印影が押したかった場所からずれる	(H3-1)印影の位置が分かりにくい	(SC3-1)印影の位置を分かり易くするようにしなければならない
(A4)印影が薄くなる	(H4-1)スタンプにインクを付けない	(SC4-1)スタンプにインクを付け忘れないようにしなければならない
	(H4-2)スタンプ台のインクが不足する	(SC4-2)スタンプ台のインクが不足することを避けなければならない
	(H4-3)スタンプをスタンプ台に不十分につけ，インク付着量が不足する	(SC4-3)スタンプを十分にスタンプ台に付けさせるようにしなければならない
	(H4-4)押印前にインクが乾く	(SC4-4)印影が乾く前に押印するようにしなければならない
(A5)印影がにじむ	(H5-1)スタンプを強く押下する	(SC5-1)スタンプを強く押下させないようにしなければならない
	(H5-2)スタンプをスタンプ台に余分につけ，インク付着量が過多になる	(SC5-2)スタンプをスタンプ台に付け過ぎないようにしなければならない
(A6)印影が汚れる	(H6-1)スタンプ台の面にゴミが付着している	(SC6-1)スタンプ台の面は綺麗に保つようにしなければならない



発表内容

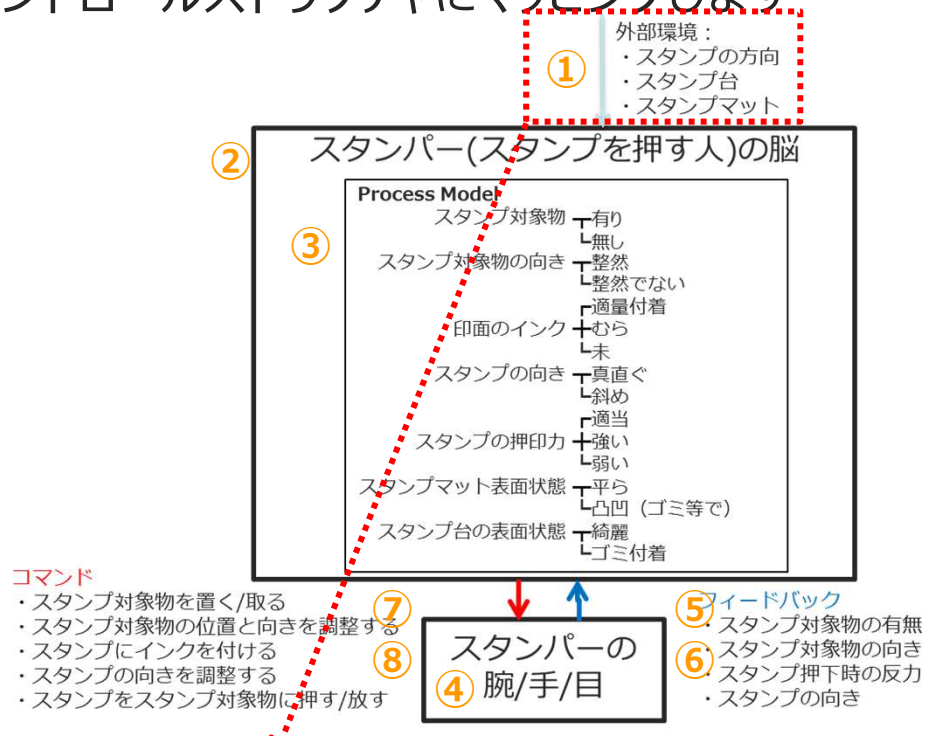
OMRON
Sensing tomorrow™

1. 背景
2. STAMPとは？
3. Step0 準備1：アクシデント，ハザード，安全制約の識別
4. Step0 準備2：コントロールストラクチャー
5. Step1：非安全なコントロールアクション(UCA)の抽出
6. Step2：HCFの特定
7. まとめ

Step2：HCFの特定

■ まずは，11個のヒントワードをコントロールストラクチャにマッピングします

ヒントワード(11個)：
①コントロール入力や外部情報の誤りや喪失
②不適切なコントロールアルゴリズム(作成時の欠陥，プロセスの変更，誤った修正や適用)
③不整合，不完全，または不正確なプロセスモデル．不適切な操作．
④コンポーネント不具合．経年変化による変化．
⑤不適切なフィードバック，あるいは，フィードバックの喪失．フィードバックの遅れ．
⑥不正確な情報供給，または情報の欠如．測定の不正確性．フィードバックの遅れ．
⑦操作の遅れ．
⑧不適切な無効なコントロールアクション，コントロールアクションの喪失．
⑨コントロールアクションの衝突．プロセス入力の喪失または誤り．
⑩未確認，範囲外の障害．
⑪システムにハザードを引き起こすプロセス出力



■ マッピングしたヒントワードから，HCFの特定を行います

◆(SC1-1)“印面は平らにしなければならない”に対する違反
➢ (CA4-P1)スタンパーが，印面が平らでないスタンプに，インクを付ける／SC1-1違反
シナリオCA4-P1-1/①コントール入力や外部情報の誤りや喪失：スタンプをもとの場所に戻す時，突起がある個所に印面を置き，印面に凹凸ができる
■対策：スタンプ設置場所には，突起物はなるべくなくし，適切なスタンプ置き場所を設置する．
■対策：スタンプ押印後は，スタンプ置き場所に戻すようガイダンスする．

Step2：HCFの特定

◆(SC1-2) “印面にインクを均一につけなければならない”に対する違反
- (CA4-P2)スタンパーが，スタンプ台の表面が綺麗でスタンプの押印力が適切に，スタンプにインクを付ける(？印面に均一につかない)
  - シナリオCA4-P2-1/①コントール入力や外部情報の誤りや喪失：スタンパーは，印面を均一にスタンプ台に付けられない.
    - ■対策：印面を細かく，軽く，叩くようにスタンプ台に付け，印面にまんべんなく均一にインクを付けるようにガイダンスする.
  - シナリオCA4-P2-2/①コントール入力や外部情報の誤りや喪失：スタンプ台に含まれているインクが場所によって斑がある.
    - ■対策：印面にインクを付けるときは，印章を回転させながら，またスタンプ台にあたる部分を変えながら，細かく軽く叩くようにガイダンスする.

◆(SC1-3) “スタンプマットの面は平らにしなければならない”に対する違反
- (CA1-P1)スタンパーが，スタンプマット表面上に凹凸があるところに，スタンプ対象物を置く
  - シナリオCA1-P1-1/①コントール入力や外部情報の誤りや喪失：スタンプマットにシールがついていたり，薄い物が置かれた状態で，スタンプを押す.
    - ■対策：スタンプ対象物をスタンプマット上に置く際は，マット上のごみ等を取り除くようにガイダンスする.

◆(SC1-4)“スタンプマット上の物を取り除かなければならない”に対する違反
- (CA1-P2)スタンパーが，スタンプマット上に物が置かれているところに，スタンプ対象物を置く
  - “シナリオCA1-P1-1”と同じ

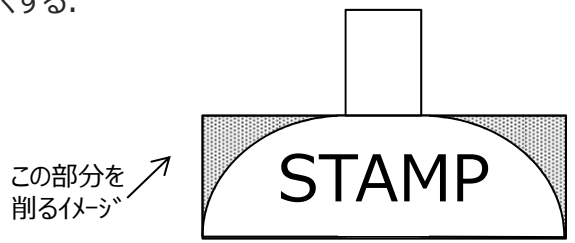
◆(SC1-5) “(押印時)印面に均一に押印力がかかるようにしなければならない”に対する違反
- (CA6-P2)スタンパーが，スタンプをスタンプ対象物に押す（？印面部に均一に押印力がかからない)
  - シナリオCA6-P2-1/③不整合，不完全，または不正確なプロセスモデル．不適切な操作：印面に均一に力を掛っている事の判断が難しく，印面に均一に力を掛けられなかった.
    - ■対策：押印時に，印章を上げる前に印面の外周に沿わすように力を掛けるように印章をくるっと回すようガイダンスする.

Step2：HCFの特定

◆(SC2-1) “印章の上下方向を分かり易くするようにしなければならない”に対する違反
- (CA5-P1)スタンパーが，スタンプの向きが斜めの時，印面の向きを調整する（？調整量不足）
  シナリオCA5-P1-1/①コントール入力や外部情報の誤りや喪失：スタンパーは，印面をみても分かりにくく，上下しるしがあっても気づかず逆さに押してしまう.
  ■対策：アクリル製にし，スタンプの印影がアクリル印面方向に見えるようなスタンプにする.

◆(SC2-2) “スタンプ対象物を整然と置かれるようにしなければならない”に対する違反
- (CA3-NP1)スタンパーが，スタンプ対象物が整然と置かれてない時に，スタンプ対象物の位置と向きを調整しない
  シナリオCA1-P2-1/①コントール入力や外部情報の誤りや喪失：スタンパーは，スタンプ対象物に正対できず，スタンプを綺麗に押せない
  ■対策：スタンプマットの上辺部にガイド(凸部)を設けスタンプ対象物が整然と置けるようにし，
  スタンプマットのガイドに沿って，スタンプ対象物を置くようにガイダンスする.

◆(SC3-1) “印影の位置を分かり易くするようにしなければならない”に対する違反
- (CA6-P1)スタンパーが，スタンプをスタンプ対象物に押す（？印影位置不認識）
  シナリオCA6-P1-1/①コントール入力や外部情報の誤りや喪失：スタンパーは印章に厚みがある為，印影ができる部分を正確に把握できず，印影の位置がずれてしまう.
  ■対策：印章を中心部から外周部に掛けて薄くする.



Step2：HCFの特定

◆(SC4-1) “スタンプにインクを付け忘れないようにしなければならない”に対する違反
- (CA4-NP1) スタンパーが，スタンプにインクをつけない
  シナリオCA4-NP1-1/⑧不適切な無効なコントロールアクション，コントロールアクションの喪失：スタンパーは，スタンプ台にスタンプをつけ忘れたまま，押印する.
  ■対策：位置関係を右からスタンプ，スタンプ台，スタンプマットとする（右利き仕様ですが．．．）

◆ (SC4-2) “スタンプ台のインクが不足することを避けなければならない”に対する違反
- (CA4-P3)スタンパーが，スタンプ台の表面が綺麗でスタンプの押印力が適切に，スタンプにインクを付ける(？インク量不足)
  シナリオCA4-P4-1/①コントール入力や外部情報の誤りや喪失：スタンプ台のインクが足りず，スタンプ台に押しつけても十分なインクが付かない
  ■対策：定期的にスタンプ台をメンテナンス（インクの補充）をする.

◆(SC4-3) “スタンプを十分にスタンプ台に付けさせるようにしなければならない”に対する違反
- (CA4-D1)スタンパーが，スタンプにインクを付ける時間が短かすぎる
- (CA4-P4)スタンパーが，押印力を弱で，スタンプにインクを付ける
  シナリオCA4-D1-1/⑧不適切な無効なコントロールアクション，コントロールアクションの喪失：スタンパーは，スタンプをスタンプ台にちょっと付けただけで，押印した.
  ■対策：UCA(CA4-P2)の対策で代用

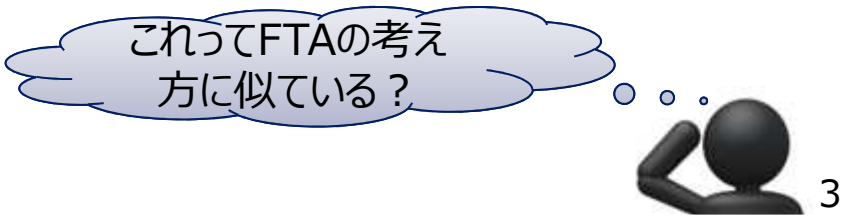
◆(SC4-4) “印影が乾く前に押印するようにしなければならない”に対する違反
- (CA6-T1)スタンパーが，スタンプをスタンプ対象物に押すのに時間がかかり過ぎる(インクが生乾き)
  シナリオCA6-T1-1/⑦操作の遅れ：スタンプ台から付けたインクが，スタンプを押す前に乾いてしまった.
  ■対策：速乾性のインクは使わない.

Step2：HCFの特定

◆(SC5-1) “スタンプを強く押下させないようにしなければならない”に対する違反
- (CA4-P5)スタンパーが，押印力を強で，スタンプにインクを付ける
  シナリオCA4-P2-1/⑧不適切な無効なコントロールアクション，コントロールアクションの喪失：スタンパーは必要以上にスタンプを押し過ぎた
  ■対策：UCA(CA4-P2)の対策で代用

◆(SC5-2)“スタンプをスタンプ台に付け過ぎないようにしなければならない”に対する違反
- (CA4-D2)スタンパーが，スタンプにインクを付ける時間が長すぎる
  シナリオCA4-D1-1/⑧不適切な無効なコントロールアクション，コントロールアクションの喪失：スタンパーが，スタンプ台にスタンプを沢山付け過ぎた為，印影が滲んだ.
  ■対策： UCA(CA4-P2)の対策で代用

◆(SC6-1)“スタンプ台の面は綺麗に保つようにしなければならない”に対する違反
- (CA4-P6)スタンパーが，スタンプ台にゴミ類が付着した状態で，スタンプにインクを付ける
  シナリオCA4-P6-1/①コントール入力や外部情報の誤りや喪失：スタンプ台にゴミ類が付着していたが，それを取り除かずにスタンプ台にスタンプを付けた為，そのゴミがスタンプ面に移ってしまい，ゴミが付着した印影となった.
  ■対策：定期的にスタンプ台をメンテナンス（スタンプ台の面を清掃）をする.



STPAで分かった，綺麗な印影にする方法！

■ 対策から導いた綺麗な印影に仕上げる方法：

○スタンプ台の使い方：
1. 細かく，軽く，叩くようにスタンプをつける.
2. スタンプを回転させながら，スタンプ台にあたる場所を変えながらつける.

○スタンプの押し方：
1. スタンプをスタンプ対象物に軽く押し，スタンプの外周に沿って力が掛かるようにレバーを回すイメージで，スタンプに軽く力をかける.

発表内容

OMRON
Sensing tomorrow™

1. 背景
2. STAMPとは？
3. Step0 準備1：アクシデント，ハザード，安全制約の識別
4. Step0 準備2：コントロールストラクチャー
5. Step1：非安全なコントロールアクション(UCA)の抽出
6. Step2：HCFの特定
7. まとめ

Step1を“システマチック手法”をやってみて感じたこと

OMRON
Sensing tomorrow™

■ Generalな手法と比べると，
- UCA構文をもちいる事で，ソースコントローラとコントロールアクション，コンテキスト，タイプが明確となり，“UCAとは何か”が明確となった
- UCA表をまとめる際に，4カテゴリのどこに記入するか迷わなくなった
- UCAとなるコンテキストの分析の網羅性が向上した

■ 今後の改善点
- コンテキストの条件を抽出する手法の工夫が必要
- UCA構文を日本文にすると違和感がでてしまうので，UCA表現方法に工夫が必要
- コンテキストの条件(コンテキスト変数・値)が増加すると，コンテキスト表の作成に時間がかかるので，ツール(Excelマクロ等)で自動生成できるとよい

⇒ Step2のシステマチック手法が出てくることを待ち望まれますが．．．
Step2は，FTA・FMEA経験者であればハードルはそれほど高くない

といえば．．．

STPAの良さ

従来の手法より多くのハザード発生原因を特定できたという話を聞いているが，

FTAとFMEAの良さを兼ね備えた安全解析手法

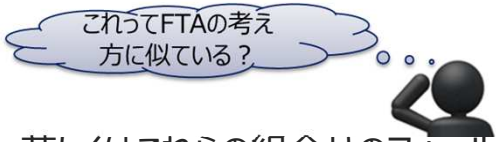
■ STEP1の最後のスライドで：

- FMEA：設計の不完全や潜在的な欠点を見出すために構成要素の故障モードとその上位アイテムへの影響を解析する技法（Wikipediaより）
  ⇒構成要素の故障モードから，アイテムの機能不全を解析する（危険状況になるコンテキストが加わるとアクシデントとなる）

構成要素を“CS図のCA”，故障モードを“4つのガイドワード”とした際，CAの故障モードからハザードを解析している構造となっている（ハザードを引き起こす故障モードがUCA）
いわゆるボトムアップ手法の考え方に似ている

- さらに，FMEAの課題を克服：
  FMEAを行う際に，部品が故障すると“過去にあったトラブルが発生するか”に焦点をあててしまいがち
  ⇒STPA Step0で思考を柔軟にし，STEP 1 でハザードを発散的に解析する

FMEA本来の機能不全を発散的に解析するという良い点



■ STEP2の最後のスライドで：

- FTA：下位アイテム又は外部事象、若しくはこれらの組合せのフォールトモードのいずれが、定められたフォールトモードを発生させ得るか決めるための、フォールトの木形式で表された解析（Wikipediaより）
  ⇒これだけは発生させたくないという事象を深堀していく解析手法

深堀していく考え方がまさにトップダウン手法の良い点

OMRON

Sensing tomorrow™

ご清聴ありがとうございます