IPA Better Life with IT

人・組織に関わるHCF特定のためのヒントワードの提案

Proposal of “Hint words” for identifying hazard causal factors in case of systems including human and/or organization.

2016年12月7日

独立行政法人　情報処理推進機構
ソフトウェア高信頼化センター
三原　幸博

目　　次（Agenda）

背景　background

- ネットワークを通じてシステムが連携する新たなサービス拡大
- 新たなシステムの基幹を担う要素がソフトウェア中心に変化
- システム相互間の複合原因によるシステム障害が増加
  - 個別視点の分析に留まっている
  - 原因分析が充分にできていない

要　求

- 複数の機器や組織（人間）が、相互に作用する複雑なシステムにおいて、相互作用のハザード要因を識別可能にする。
- システム全体の振る舞いを確認しながらポイントを絞って分析可能にする。

背景

STAMP/STPAに対する期待が高まってきている

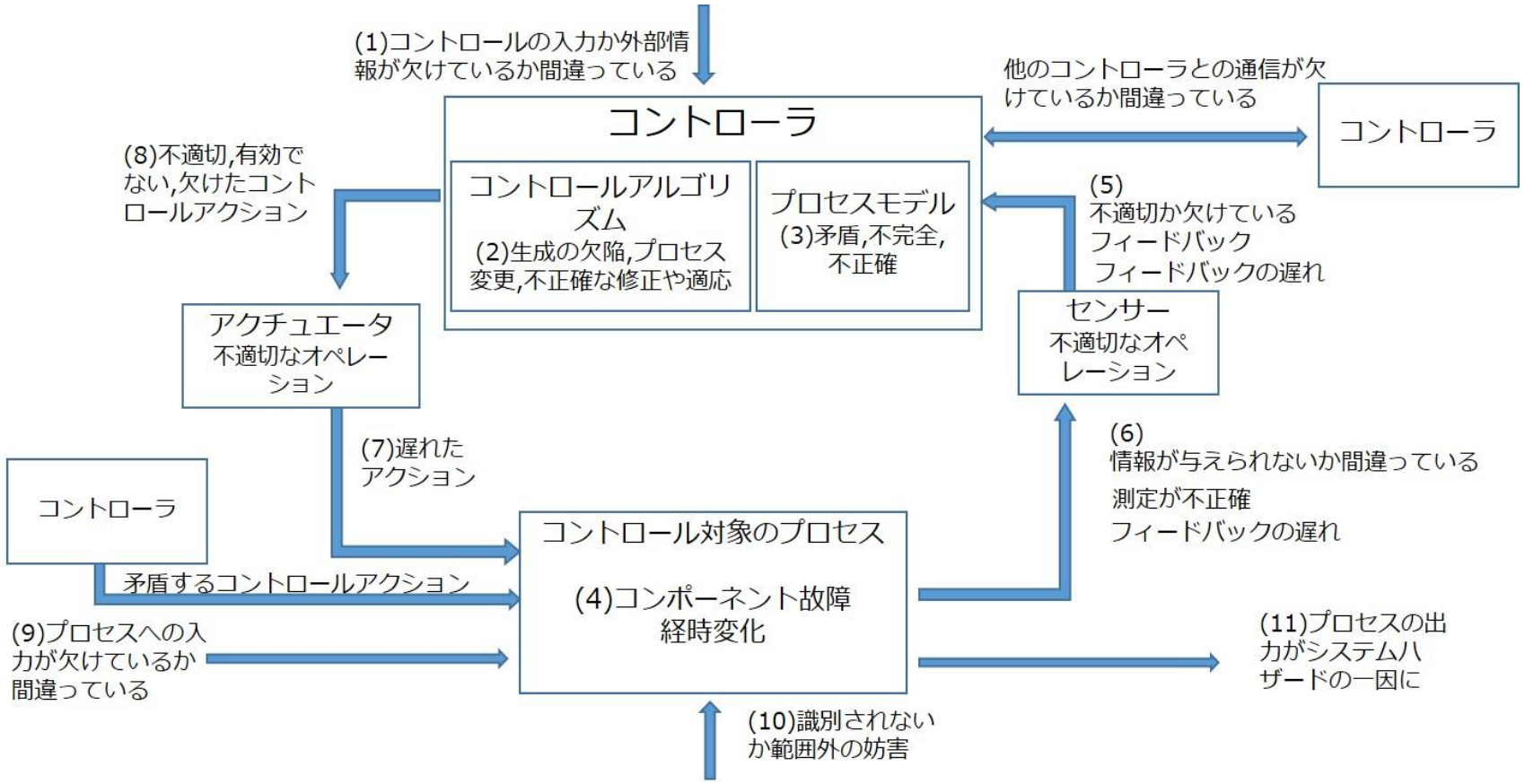
- software中心のシステムの脆弱性（リスク）を分析できる
- 自動化によるシステムの高度化等の進展により信頼性は基より安全性が重要視されてきている

STAMP/STPA活用上の課題⇒HCF(Hazard Causal Factor)特定のためのヒントワード(Hint Words)

- ヒントワードは想定外のHCFを見つけるための重要な働きをする
- ドメインエキスパートではない人が分析できるようにするにはヒントワードが必要
- 分析対象分野の共通基盤技術にヒントワードをプラスすることで解決できる可能性大
- 提示されているヒントワードが制御機械と稼働機械の組合せのみ

SEC
Software Reliability Enhancement Center

ハザード要因（HCF）を特定する際に参考にする安全制約を破られる原因の例



安全性解析を必要とするシステムの特徴

Characteristics of systems required safety analysis

人と組織と機械が協調して動作する

- 多くの重要な社会技術システムは、人と組織と機械が相互に連携している
  - ロボットによって自動化が進んだ製造現場
  - 自動操縦機能を持った航空機や鉄道
  - 運転支援機能が高度化する自動車
  - 遠隔操作や自動化が進んでいる建設機械
- 人と組織と機械が相互に干渉することで新たなリスクが懸念されている

現状
Current situation

- 人と組織をハザード要因とするアクシデントが少なくないが、要因が整理されていない

  事例：組織毎のルールの不一致と組織の対応不備による航空機事故

⇒ 人と組織の行動が事故に繋がりうるハザード要因が例示（ヒント）されていると分析の負荷が軽減される（敷居が下がる）

事故例　組織毎のルールの不一致と組織の対応不備による航空機事故

Accident 2 : Überlingen mid-air collision

SEC Software Reliability Enhancement Center

[事故概要]

2002年7月1日の21時35分 にバキシール航空2937便、乗客60人 – 大半は子供 – と乗員9人が搭乗）とDHL611便（パイロット2人が搭乗）がドイツ南部のユーリンゲン上空で衝突した事故である。両機に搭乗していた71人全員が死亡。連邦 航空事故調査局は、この事故は事故当時これらの便を監視していたスイスの**航空管制システムの欠陥**と**TCAS（航空機に搭載される衝突防止装置）が発した警報の取り扱いにおける曖昧性**により発生と発表。

[事故原因]

管制を担当していたスカイガイド社の設備に複数のトラブルが発生していた上に、管制上の規律違反が重り事故が発生。当直の管制官は2名だったが、内1人は休憩のために業務から離れており、**違反であるが、長年の慣習となっており、上層部も黙認**していた。

また、チューリヒ航空管制センターの**接近警報装置が事故の約30分前からメンテナンスのため作動していなかった**。また**主電話回線網も調整のため電源が切られており、代わりの予備回線も不調**であった。このため、運行が遅延していた別の航空機1135便の進入管制をフリードリヒスハーフェン管制塔に引き継ぐことができず、**事故の45秒前まで、1135便を進入誘導しており、この間に2機が異常に接近していることに気付かず、対処が遅れた**。ほかに地上レーダーの不使用などが原因でレーダーシステムに航空機の機影が一時的に消えたり、位置が正確に表示されない不具合も発生していた。

いずれの事故機にもTCASが装備されており、衝突の36秒前に双方のTCASが正常に作動して611便では降下、2937便では上昇の指示をそれぞれの乗員に与えていたが、**611便の乗員がTCASの指示に従って管制承認高度を離脱し降下を開始した**一方で、**2937便の乗員はTCASを無視し管制官の指示に従って降下を開始した**ことが明らかになった。加えて、TCASの指示が出ていることを知る術は管制官にはなく、611便がTCASの指示に従って降下中であることを無線で連絡しようとするも混信で失敗したために、**管制官は、611便が管制承認高度36,000フィートを維持しているものと信じて**2937便に緊急降下を指示し、両便とも降下していることに最後まで気づかなかった

人と組織のヒントワードの要件

Requirements for Hint Words about human and/or organization

SEC Software Reliability Enhancement Center

- 網羅性
  - UCAのガイドワードに対応
    (Not Providing/Incorrectly Providing,too early,too long)
- 現実的
  - 人間の生物的特性に沿っていること(視覚/聴覚/触覚)
  - 人間の生理的特性に沿っていること(集中力/記憶力/精神力/生理現象)
  - 善意/悪意/恐怖/圧力
  - 環境条件を含む
- 対策実現性
  - 技術的実現性
  - 業務ワークフローの実行可能性

アプローチ
Approach

- 事故事例調査/収集と教訓化活動から得られたハザード要因を整理

（IPA/SEC 情報処理システム高信頼化教訓集2015年度版）

- コントロール側をNot Providing/Incorrectly Providing に、被コントロール側をコミッション/オミッションに対応づけて整理
- M-SHELモデルを参照して規定等と環境に関する要因を整理

人と組織と機械が絡み合ったシステムのコントロールループを考えるとSTAMP/STPAとM-SHELの要素は以下のように対応付ける事ができる。

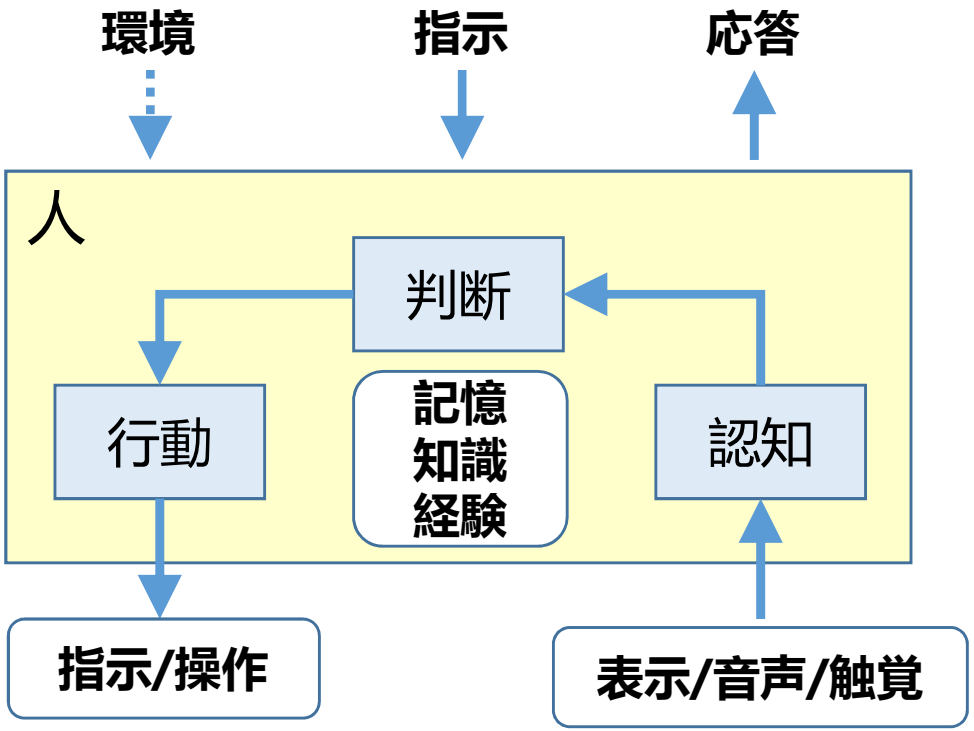
STAMP/STPA	M-SHEL
コントローラ	L
コントロール対象	L,H
コントロールアルゴリズム	M
プロセスモデル	S
全体への影響	E

- 人間工学を参照

M-SHELモデル：（出典：日本ヒューマンファクター研究所）
機械やシステムを安全に、有効に機能させるために必要とされる人間の能力や限界、特性等のヒューマンファクターを表現するためのモデル。
中央のL：（当事者）
H：ハードウェア：（機器、機材、設備、等）
M：マネジメント：（コミットメント、体制、分担、リスク管理、等）
Sソフトウェア（規程、規則、細則、要領、等）
E：環境（気温、湿度、換気、騒音、照明、空間、遠近、利便、安全文化、風土、慣習、等）
L：（相手、関係者、第三者）

人間工学を参照　reference of human engineering

人と組織の関与を考えるにあたって、「認知」「判断」「行動」、「環境」において、ハザードにつながる要因を見出すヒントを与えることで整理できる



「認知」に対して考えられる要因

表示など出力を欠落させる

正しい/正しくない出力を間違って認知する

「行動」に対して考えられる要因

正しくない指示を出す

指示を出さない

- 「判断」に対して考えられる要因

指示/操作を忘れる、必要と思わない　意図的/無意識

指示/操作を勘違い/考え違いする

指示済み/思い込み

- 「環境」が人に対して与える要因

誤った判断を引き起こす人的因子（コミュニケーションエラー）

連絡不足/報告不足/確認不足/公開不足/隠蔽/複雑な手順

誤った判断を引き起こす精神的因子

プレッシャー/規制強化/社会通念/事故感受性の不足

視覚・聴覚の妨害/錯覚

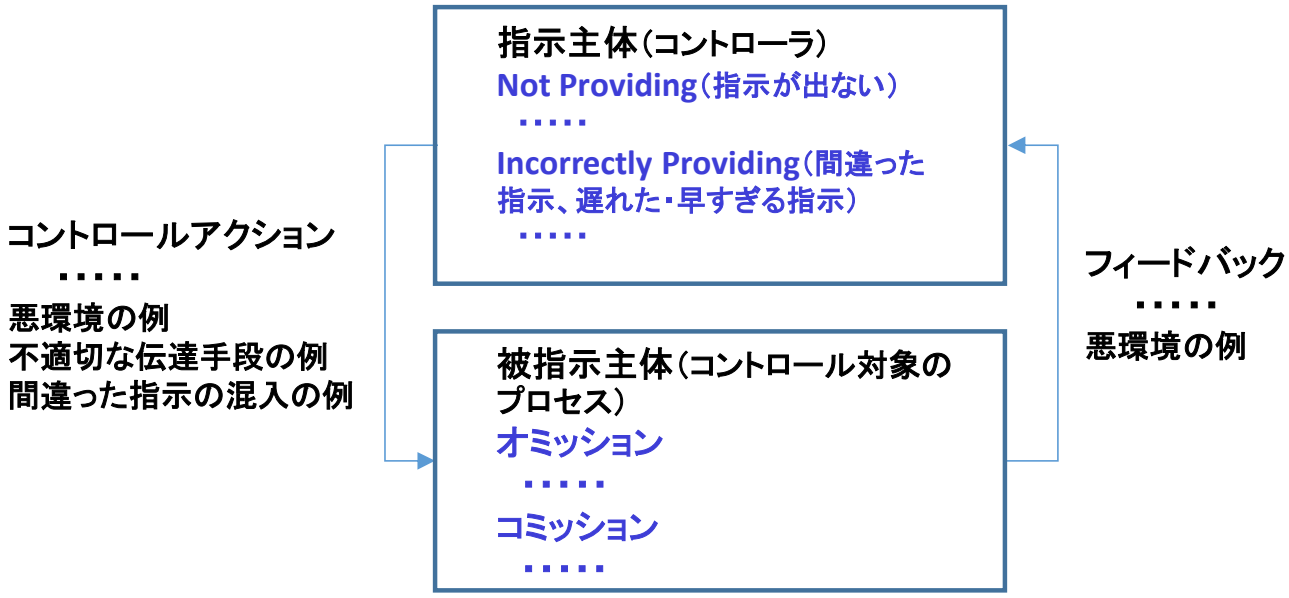
＊「原子力分野におけるリスク評価とヒューマンエンジニアリング」第４回リスク学研究会、平成21年3月28日（財）エネルギー総合工学研究所氏田博士

＊情報技術と倫理第１０回講義「ヒューマンエラーとユーザインタフェース」大阪大学　清川清教授

情報処理レベル（認知心理的分類）橋本(1981) の分類/Norman (1988) の分類

ヒントワードの組合せ

- (人) 対 (人) のHCF導出のためのヒントワード
- (人) 対 (機械) のHCF導出のためのヒントワード
- (機械) 対 (人) のHCF導出のためのヒントワード （省略）
- (組織) 対 (人) のHCF導出のためのヒントワード
- (人) 対 (組織) のHCF導出のためのヒントワード （省略）
- (組織) 対 (組織) のHCF導出のためのヒントワード



（人）対（人）のHCF導出のためのヒントワード

Hint Words identifying HCF of human to human

SEC Software Reliability Enhancement Center

不適切な伝達手段の例
- *不適切な信号発光（形状、色）*
- *指差呼称、復誦などのしつけ不足*
- *一方的な伝達（多数のFAX送信など）*

間違った指示の混入の例
- *意図的な改ざん*
- *類似標識の混在*
- *類似伝達手段の混在*

指示（口頭・電話・メイル・FAXなど光、音、旗）

(A1)指示が伝わらない（悪環境で阻害/伝達手段故障/不適切な伝達手段）
(A2) 指示が遅れる
(A3)間違った指示の混入

悪環境の例

発光を認識できない理由
- *雪、雨、霧による視界不良*
- *逆光が強い*
- *線路が大きくカーブしている*
- *途中にトンネルがある*
- *途中に遮蔽物（木など）がある*
- *不適切な装備（サングラスなど）*
- *騒音で聞こえない*

指示主体（人）

Not Providing（指示が出ない）
(HC1)指示が必要と思っていない
(HC2)指示を知っていたが忘れる
(HC3)指示したつもり
(HC4)フィードバックを見逃して操作をしない
Incorrectly Providing（間違った指示、遅れた・早すぎる指示
(HC5)指示内容を間違える
(HC6)思い出す（遅れる）
(HC7)指示内容を勘違い（取り違える）
(HC8)違う相手に指示を出す
(HC9)フィードバックを誤解して間違った操作を行う
(HC10)確認せずに見込みで指示を出す

被指示主体（人）

オミッションエラー
(HP1)指示が来たが受け取らない
(HP2)指示が来たがスキル不足で実施できない
(HP3)実行結果のフィードバックを忘れる
コミッションエラー
(HP4)指示を誤解して実行する
(HP5)指示どおりの実行ができないまたは遅れる
（不適切な環境、スキル不足、健康状態不良）
(HP6)思い出す（遅れる）

フィードバック（口頭・電話・メイル・FAXなど）

(F1)フィードバックが伝わらない（悪環境で阻害/伝達手段故障/不適切な伝達手段）
(F2)フィードバックの遅れ
(F3)間違ったフィードバック
(F4)フィードバックでない

（人）対（機械）のHCF導出のためのヒントワード

Hint Words identifying HCF of human to machine

SEC Software Reliability Enhancement Center

指示主体（人）

Not Providing（操作忘れ）
(HC1)指示が必要と思っていない（知識不足）
(HC2)指示を知っていたが忘れる（多忙、訓練不足、体調不良）
(HC3)指示したつもり（訓練不足、確認手順が不適切）
(HC4)フィードバックを見逃して操作をしない
Incorrectly Providing（操作ミス）
(HC5)指示内容を間違える（知識不足、訓練不足）
(HC6)思い出す（遅れる）（訓練不足、体調不良）
(HC7)指示内容を勘違い（取り違える）（訓練不足）
(HC8)違う相手に指示を出す（知識不足、訓練不足）
(HC9)フィードバックを誤解して間違った操作を行う
(HC10)確認せずに見込みで指示を出す

被指示主体（機械）

オミッションエラー
(MP1)指示が来たが受け取れない（故障）
コミッションエラー
(MP2)指示どおりの実行ができないまたは遅れる（故障又は不適切なアルゴリズム）
(MP3)間違った指示で対応できない

指示（操作：SW,KB）

(A1)指示が伝わらない（故障）
(A2)指示が遅れる（故障）
(A3)間違った指示の混入

悪環境の例
発光を認識できない理由
・雪、雨、霧による視界不良
・逆光が強い
・線路が大きくカーブしている
・途中にトンネルがある
・途中に遮蔽物（木など）がある
・不適切な装備（サングラスなど）
・騒音で聞こえない

フィードバック（画像、ランプ、音声など）

(F1)フィードバックが伝わらない（悪環境で阻害、指示手段が不適切など）
(F2)フィードバックの遅れ
(F3)間違ったフィードバック

（組織）対（人）のHCF導出のためのヒントワード

Hint Words identifying HCF of organization to human

SEC Software Reliability Enhancement Center

指示主体（組織）

Not Providing（指示が出ない）
(AC1)ミッションではない
(AC2)基準が曖昧で指示出さない
(AC3)担当者/責任者不在で判断できず
(AC4)担当者曖昧で指示出さない
(AC5)結果が不安で指示出さない
(AC6)担当者がスキル不足で状況を理解できず指示出さない（知識不足、曖昧な知識、不安、訓練未熟）で指示出さない
(AC7)担当者が別件で忙しくて指示出さない
Incorrectly Providing（間違った指示が出る、遅れる）
(AC8)基準が曖昧で指示遅れる
(AC9)基準が曖昧で間違った指示を出す
(AC10)間違った組織に指示を出す

被指示主体（人）

オミッションエラー
(HP1)指示が来たが受け取らない
(HP2)指示が来たがスキル不足で実施できない
(HP3)実行結果のフィードバックを忘れる
コミッションエラー
(HP4)指示を誤解して実行する
(HP5)指示どおりの実行ができないまたは遅れる
（不適切な環境、スキル不足、健康状態不良）
(HP6)思い出す（遅れる）

指示（口頭・電話・メイル・FAXなど光、音、旗）

(A1)指示が伝わらない（悪環境で阻害/伝達手段故障/不適切な伝達手段）
(A2)指示が遅れる
(A3)間違った指示の混入

悪環境の例
発光を認識できない理由
・雪、雨、霧による視界不良
・逆光が強い
・線路が大きくカーブしている
・途中にトンネルがある
・途中に遮蔽物（木など）がある
・不適切な装備（サングラスなど）
・騒音で聞こえない

フィードバック（口頭・電話・メイル・FAXなど）

(F1)フィードバックが伝わらない（悪環境で阻害、伝達手段故障/不適切な伝達手段）
(F2)フィードバックの遅れ
(F3)間違ったフィードバック
(F4)フィードバックでない

（組織）対（組織）のHCF導出のためのヒントワード

Hint Words identifying HCF of organization to organization

SEC Software Reliability Enhancement Center

不適切な伝達手段の例
- *不適切な信号発光（形状、色）*
- *指差呼称、復誦などのしつけ不足*
- *一方的な伝達（多数のFAX送信など）*

間違った指示の混入の例
- *意図的な改ざん*
- *類似標識の混在*
- *類似伝達手段の混在*

指示（口頭・電話・メイル・FAXなど光、音、旗）

(A1)指示が伝わらない（悪環境で阻害/伝達手段故障/不適切な伝達手段）
(A2) 指示が遅れる
(A3)間違った指示の混入

悪環境の例

発光を認識できない理由
- *雪、雨、霧による視界不良*
- *逆光が強い*
- *線路が大きくカーブしている*
- *途中にトンネルがある*
- *途中に遮蔽物（木など）がある*
- *不適切な装備（サングラスなど）*
- *騒音で聞こえない*

指示主体（組織）

Not Providing（指示が出ない）
(AC1)ミッションではない
(AC2)基準が曖昧で指示出さない
(AC3)担当者/責任者不在で判断できず
(AC4)担当者曖昧で指示出さない
(AC5)結果が不安で指示出さない
(AC6)担当者がスキル不足で状況を理解できず指示出さない（知識不足、曖昧な知識、不安、訓練未熟）で指示出さない
(AC7)担当者が別件で忙しくて指示出さない
Incorrectly Providing（間違った指示が出る、遅れる）
(AC8)基準が曖昧で指示遅れる
(AC9)基準が曖昧で間違った指示を出す
(AC10)間違った組織に指示を出す

被指示主体（組織）

オミッションエラー（指示通りに実行しない）
(AP1)ミッションではないので受け取らない
(AP2)責任者/担当者不在で放置
(AP3)責任者/担当者スキル不足で放置（曖昧な対応知識、対応知識なし、不安、訓練不足）
(AP4)担当者が別件で忙しく放置
(AP5)結果が不安で放置
コミッションエラー（間違って実施）
(AP6)責任者/担当者不在で対応が遅れる
(AP7)対応の仕方が解らず誤った対応

フィードバック（口頭・電話・メイル・FAXなど）

(F1)フィードバックが伝わらない（悪環境で阻害/伝達手段故障/不適切な伝達手段）
(F2)フィードバックの遅れ
(F3)間違ったフィードバック

有効性の検証

Verification effectiveness in case study

SEC Software Reliability Enhancement Center

適用実験：JR事例（“とりこ検知”と“踏切工事”）

特定できた非安全なコントロールの原因
（Identified causes of Unsafe control）

	全HCF all	故障 Failure	設計 Design	人 (Human)		環境 Environment
				制御行動 Control	被制御行動 Controlled	
とりこ検知 CASE 1	23件	8件	5件	2件	1件	7件
踏切工事 CASE 2	40件	1件	0件	21件	8件	10件

特定できた“人と環境に関するハザード要因”は、ヒントワードに含まれている。
専門家の評価：ほぼ網羅できている

踏切工事の人・環境に関するHCF

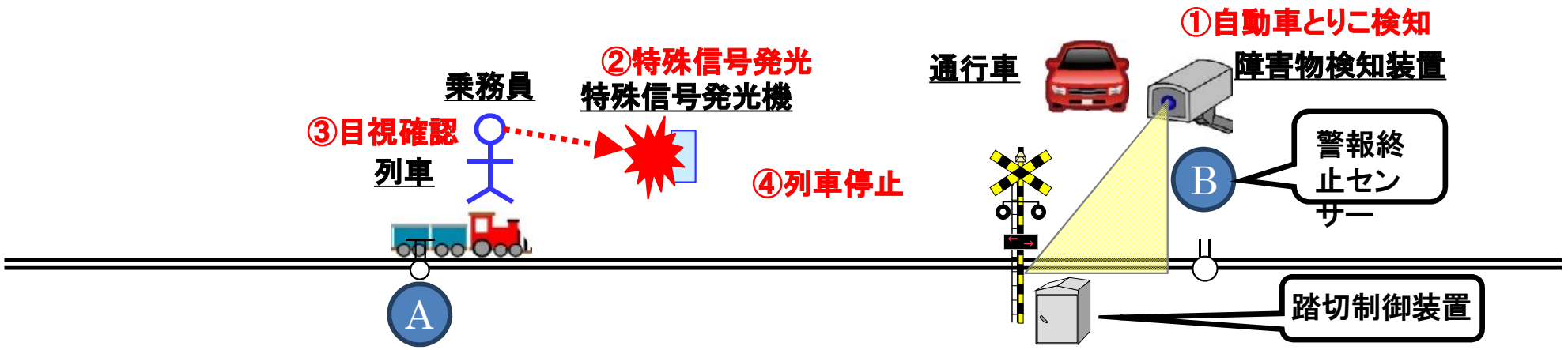
	件数
Not Providing（指示が出ない）	
(HC1)指示が必要と思っていない	3
(HC2)指示を知っていたが忘れる	2
(HC3)指示したつもり	3
(HC4)フィードバックを見逃して操作をしない	3
Incorrectly Providing（間違った指示、遅れた・早すぎる指示	
(HC5)指示内容を間違える	1
(HC6)思い出す（遅れる）	1
(HC7)指示内容を勘違い（取り違える）	1
(HC8)違う相手に指示を出す	1
(HC9)フィードバックを誤解して間違った操作を行う	1
(HC10)確認せずに見込みで指示を出す	10
オミッションエラー	
(HP1)指示が来たが受け取らない	1
(HP2)指示が来たがスキル不足で実施できない	0
(HP3)実行結果のフィードバックを忘れる	0
コミッションエラー	
(HP4)指示を誤解して実行する	3
(HP5)指示どおりの実行ができないまたは遅れる（不適切な環境、スキル不足、健康状態不良）	4
(HP6)思い出す（遅れる）	0

とりこ検知

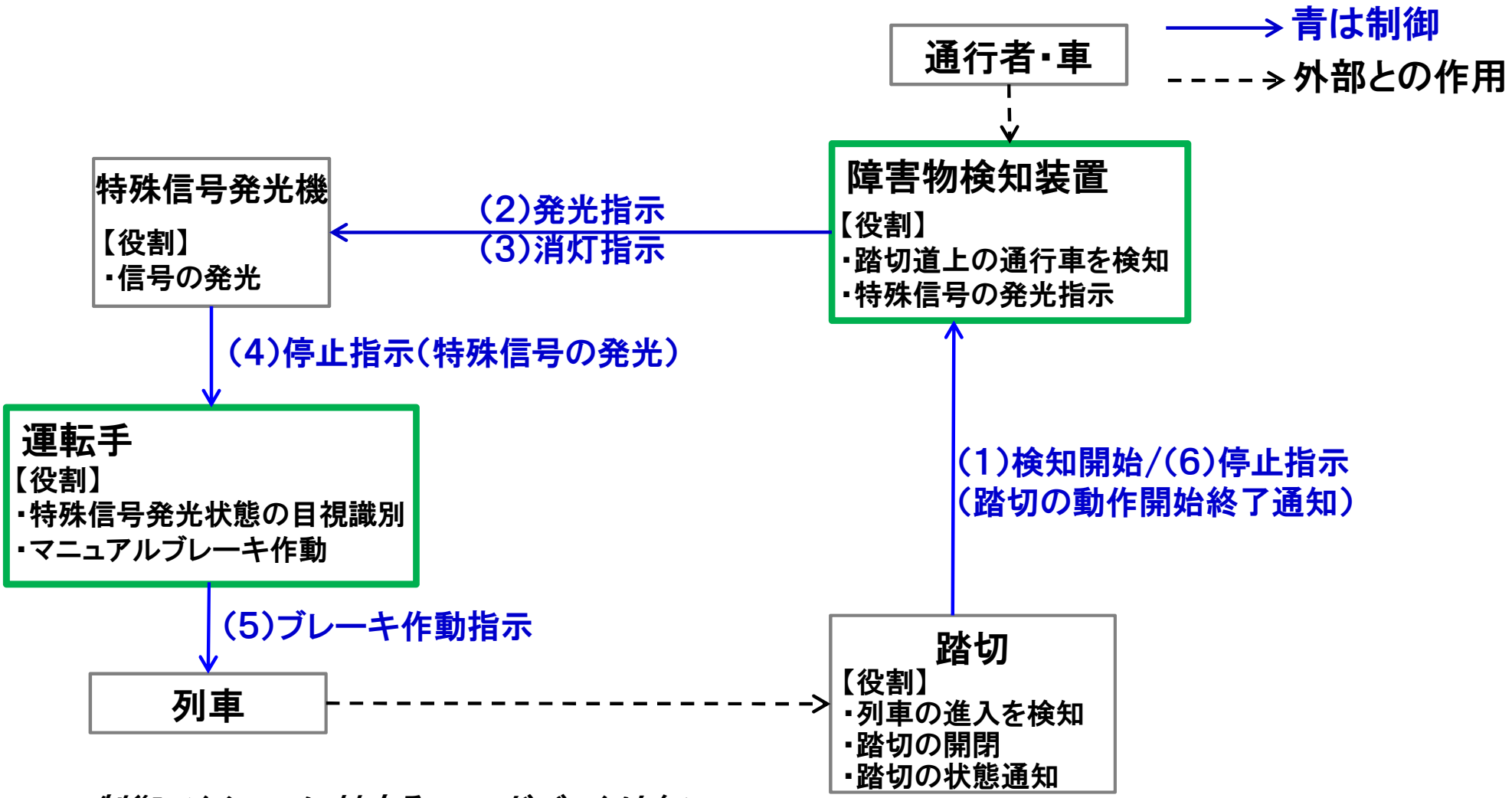
CASE 1 : Detecting cars in train crossing system

	手順	機械の動き	人の動き	備考
1	発生	踏切道上の通行車を検知	ー	
2	対応	特殊信号発光機が発光	• 乗務員が特殊信号を認識	目視による
3	対応	ー〃ー	• 乗務員が列車にブレーキをかける	マニュアルブレーキ

“とりこ検知”とは、障害物検知装置が列車の乗務員に“とりこ”を知らせてブレーキをかけさせることで踏切の安全を守るシステム(機能)である。



準備2　コントロールストラクチャの構築
Control structure



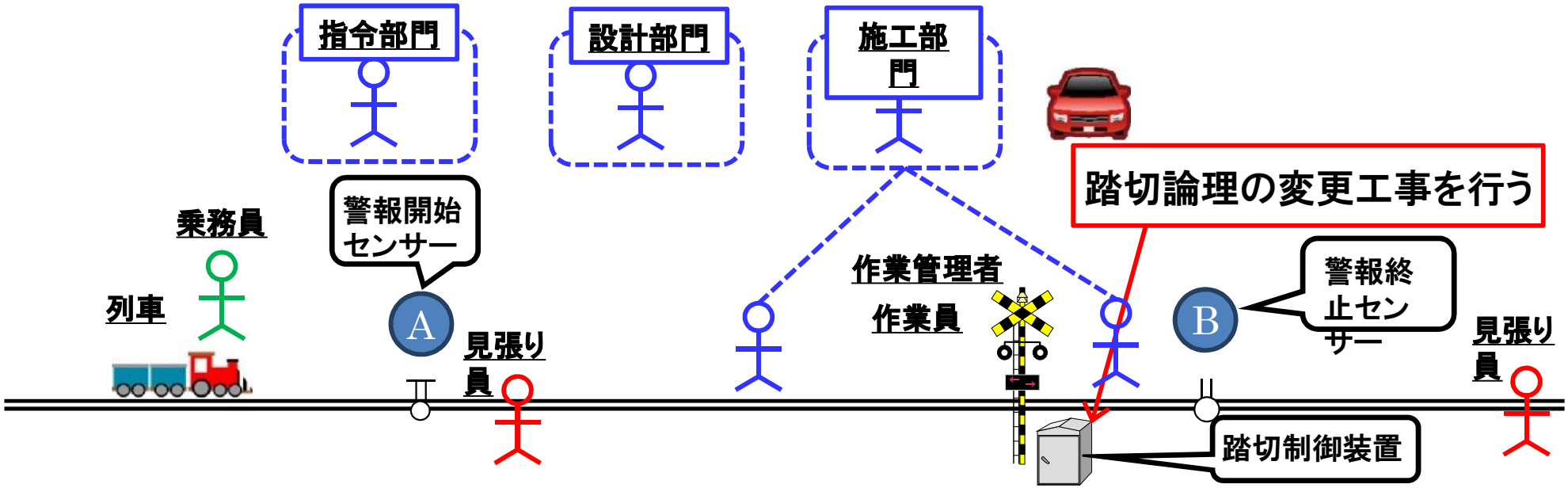
＊　*制御アクションに対するフィードバックはない*

＊＊　*メインのコントローラーは障害物検知装置で被コントロールプロセスは運転手であるが、ここでは要素間のコントロールの流れに沿って構造を記述した。*

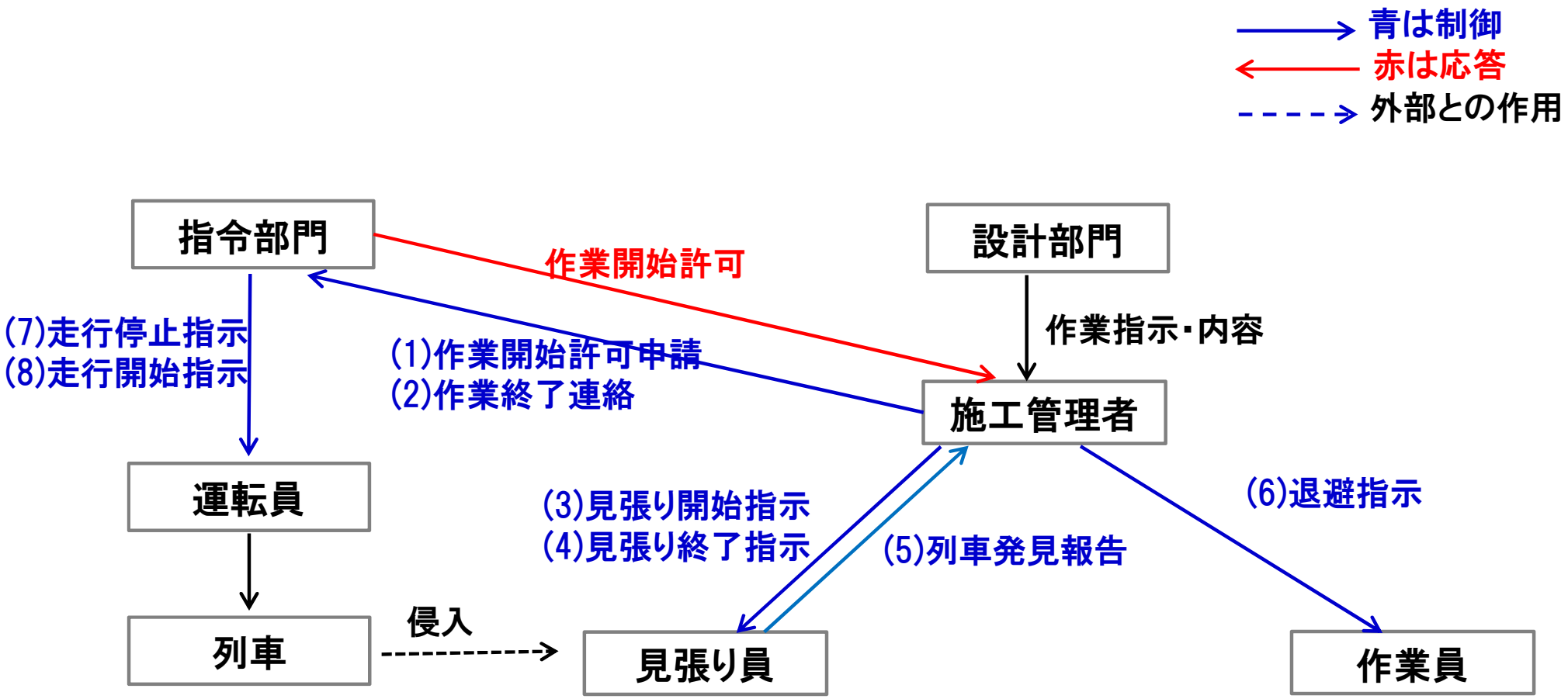
踏切工事

CASE 2：maintenance work of train crossing system

	手順	機械(踏切論理部)の動き	人の動き	備考
1	設計	ー	• 制御論理の考案 • 論理を実現する仕組み(電気配線図等)の作成	ダブルチェック、審査、承認等、人によるチェック有り
2	施工	一時使用停止(動作しない)	• 電気ケーブルの配線	目視、復唱等、人によるチェックあり
3	試験	一時使用停止(動作しない)	• 列車の模擬走行(レール短絡等)	
4	使用開始	新論理で動作	• (正常動作監視)	



コントロールストラクチャの構築
Control structure



おわりに
Conclusion

SEC
Software Reliability Enhancement Center

- 有効性の確認 ⇒　適用実験と通して有効性を確認

- 今後の課題
  - CAST事例への適用
  - 人・組織以外の知識整理方法の検討

参考文献

[1] 原子力安全・保安院電力安全課：中部電力（株）駒場堰堤洪水吐ゲートの異常作動について　平成14年04月11日（木）
http://warp.ndl.go.jp/info:ndljp/pid/286890/www.meti.go.jp/kohosys/press/0002611/
[2] 日本ヒューマンファクター研究所：品質とヒューマンファクター安心と安全の考え方、財団法人日本科学技術連盟
[3] 畑村創造工学研究所　畑村洋太郎：失敗知識データベースの構造と表現
http://www.sozogaku.com/fkd/inf/mandara.html
[4]「原子力分野におけるリスク評価とヒューマンエンジニアリング」第４回リスク学研究会、平成21年3月28日（財）エネルギー総合工学研究所氏田博士
[5]情報技術と倫理第１０回講義「ヒューマンエラーとユーザインタフェース」大阪大学　清川清教授
情報処理レベル（認知心理的分類） 橋本(1981) の分類/Norman (1988) の分類