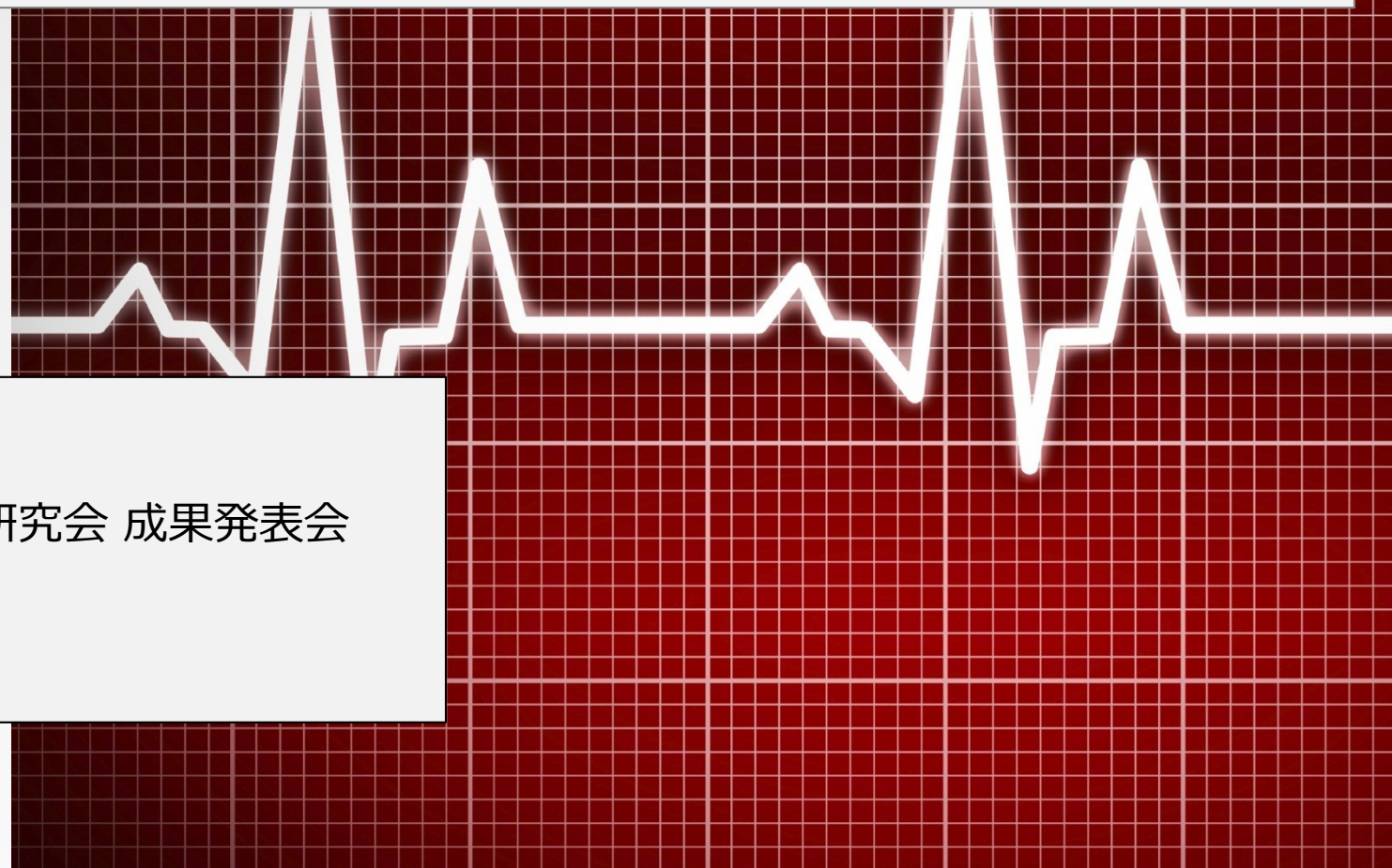
CASTと FRAMによるセキュリティ事故分析
～システム思考とレジリエンス～



一般財団法人日本科学技術連盟

第35 年度（ 2019 年度） ソフトウェア品質管理研究会 成果発表会
第８分科会 演習コースⅢ セーフティ&セキュリティ

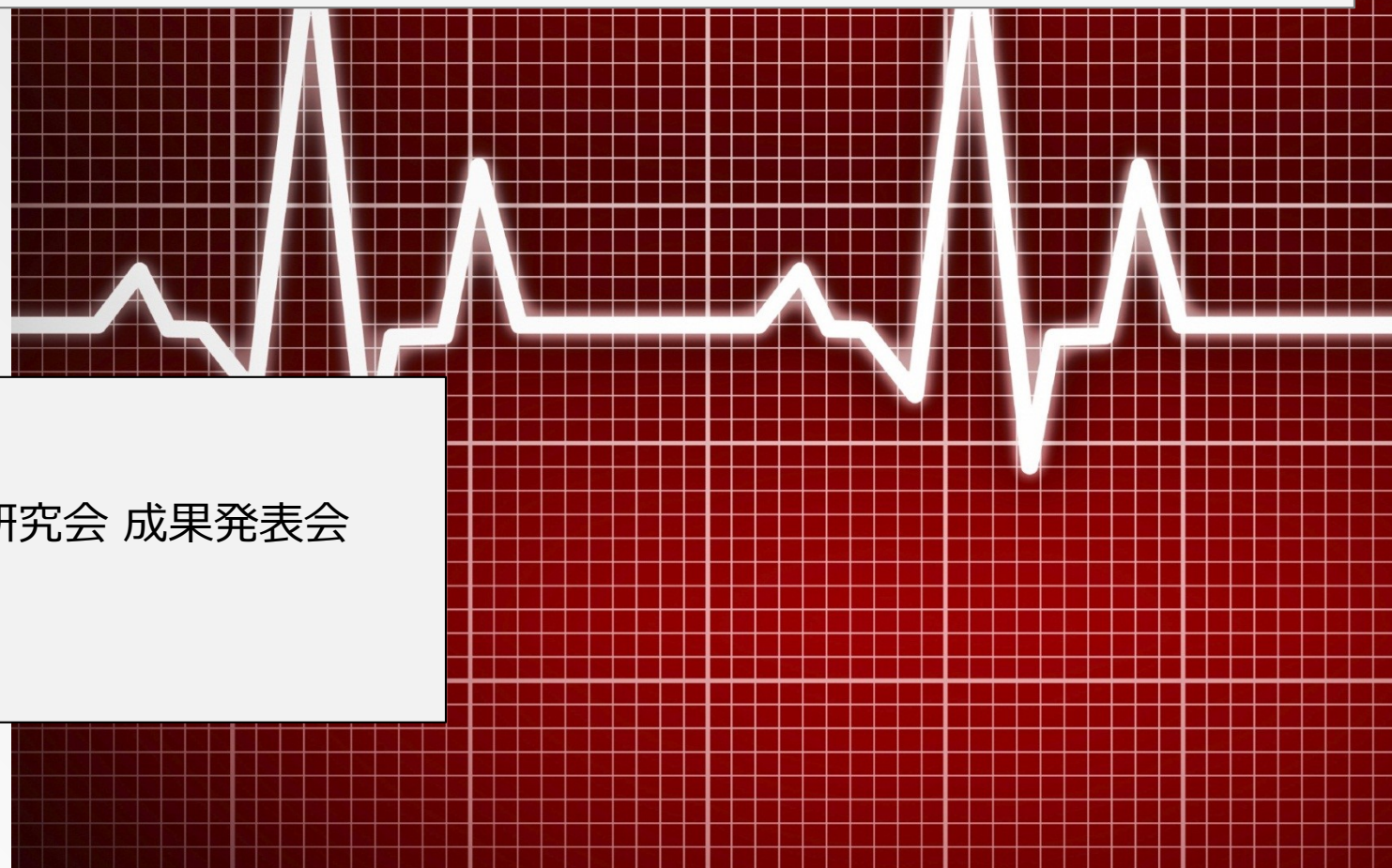
2020年2月21日

公開資料

演習Ⅲ　セーフティ＆セキュリティ2019年度実績

回	日時	講演テーマ	講演者	演習／論文作成
1	5/10	前年度実績をもとに考える「セーフティ・セキュリティ」	金子朋子	なし
2	6/14	レジリエンスエンジニアリングとFRAM	JAMSS 有人宇宙システム株式会社 野本　秀樹氏	FRAMツールを使った簡単な演習
3	7/11 7/12 （合宿）	STAMPの安全分析手法STPAと事故分析手法CAST 標準系と各種分析手法	金子朋子 髙橋　雄志	STPAとCASTの演習
4	9/12-13	ソフトウェア品質シンポジウム（臨時会　論文チーム検討）		
5	10/11	熟練経験値の継承に活かすアシュアランスケース(GSN)～ソフトウェアFMEAやFPGA設計における事例紹介～	JAXA　梅田浩貴氏	論文検討
6	11/15	スマートホームの安心安全	神奈川工科大学 一色　正夫教授	論文検討・事例化
7	12/13	IoT時代のAIと 安全性（広義のセキュリティ）	東京電機大学 佐々木良一教授	論文検討・事例化
8	1/10	AI/IoTのセーフティ・セキュリティ	金子朋子	論文作成・事例化
9	1/31	臨時会　論文作成　成果発表会準備		
10	2/21	成果発表会		

CASTと FRAMによるセキュリティ事故分析
～システム思考とレジリエンス～



一般財団法人日本科学技術連盟

第35 年度（ 2019 年度） ソフトウェア品質管理研究会 成果発表会
第８分科会 演習コースⅢ セーフティ&セキュリティ

2020年2月21日

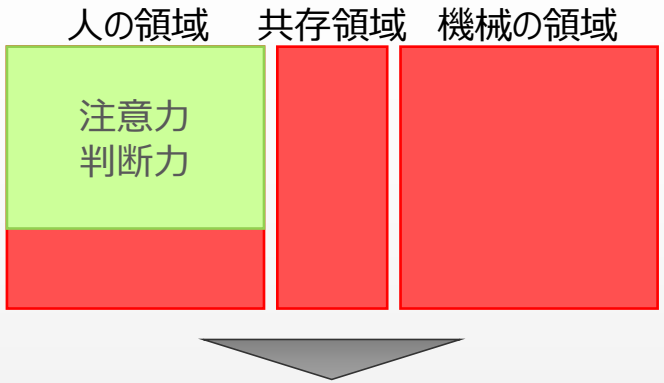
公開資料

tables of contents

セーフティ＆セキュリティの新分析手法の必要性

INTRODUCTION

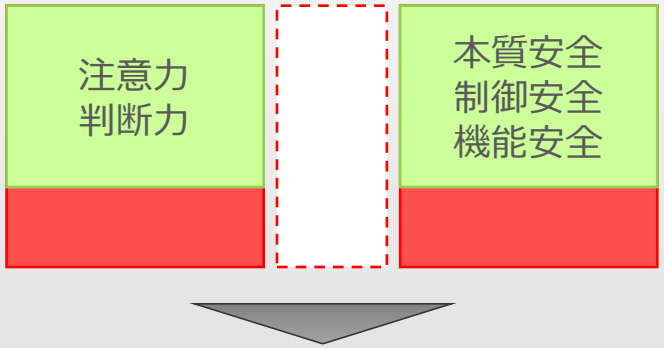
IoT時代の新しい安全 Safety2.0へ



Safety0.0 「人の注意力で安全確保」

■人による**安全**

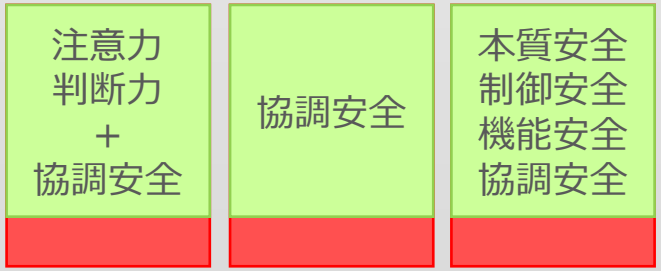
・人の領域にもリスク
・人と機械の共存領域は**リスク**
・機械の領域は**リスク**



Safety1.0 「機械技術による安全確保」

■人と機械それぞれによる**安全**

・人の領域にもリスク
・人と機械の共存領域は撤廃（隔離の安全）
・機械の領域にも**リスク**



Safety2.0 「人、モノ、環境が協調しながら安全を構築する」

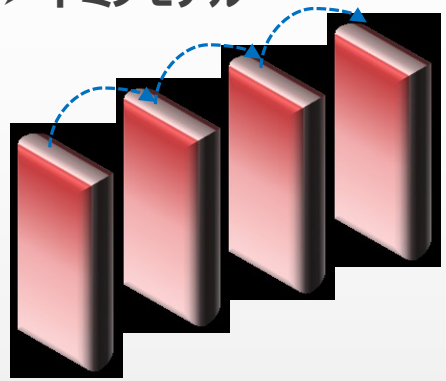
■人と機械の協調による**安全**

・人の領域のリスクを最小化
・人と機械の共存を可能に
・機械の領域の**リスク**を最小化

IoT、AIの時代を迎えるに当たり、複雑・多様化するソフトウェア
サイバーセキュリティへの対応も同時に必要とされる時代が到来

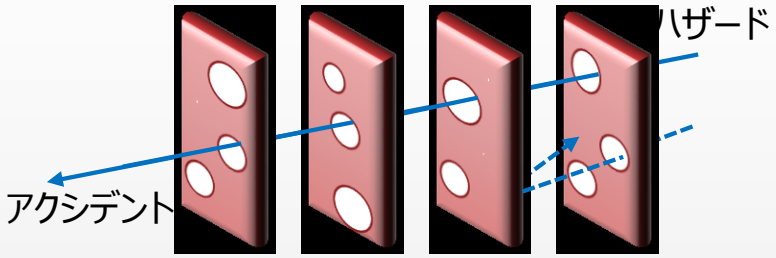
従来の事故モデルと安全分析手法

➢ **ドミノモデル**



- 原因－結果（次の原因）－…の系列をドミノ倒しにたとえるこのドミノ倒しのどこかで手を打てば事故が避けられるとする
- 根本原因分析といわれる事故分析の各手法は、この考えに立っている

➢ **スイスチーズモデル**



- 防御壁とそこでの漏れをチーズの穴にたとえる穴が重なって見通せたときに事故となる
- 個々の穴をふさぐことで対策とする

➢ **FMEA(Failure Mode and Effects Analysis)**
（還元的に）各部品・機能の故障モードがどのようにシステムに影響するかを分析する
1．故障モード（故障）の抽出が難しい
2．限られた開発工数の中でやりきれない

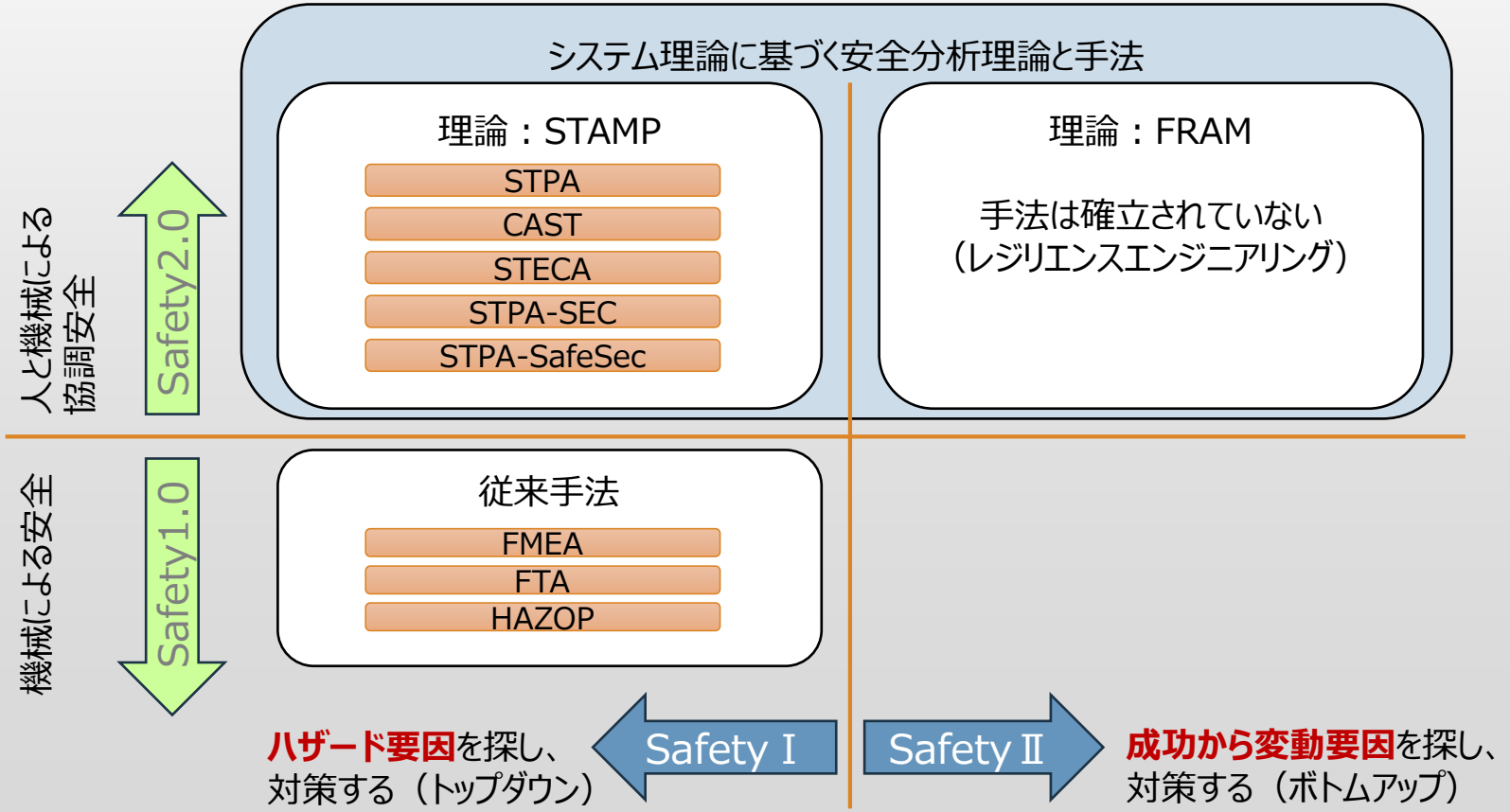
➢ **FTA（Fault Tree Analysis）**
安全上起きてはいけないことが起きていないことを検証する

➢ **HAZOP(Hazard and Operability Study)**
FMEAやFTAの中でガイドワードの考え方を用いる
※主に経験知に基づく網羅性によって安全性を論証する

従来の分析手法は、過去の事故やバグの経験、知見がないと分析困難（還元主義）

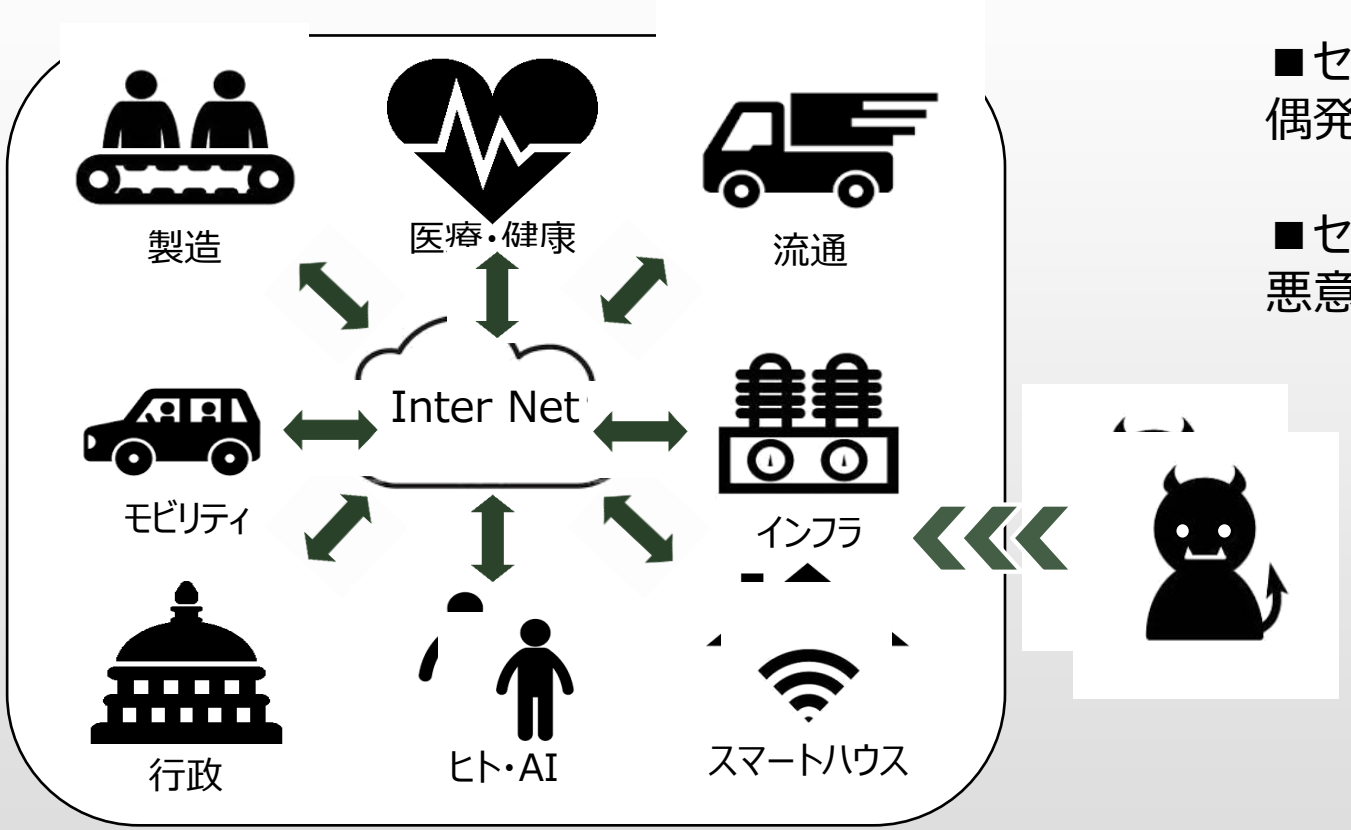
Safety-Ⅰ,Ⅱとセーフティ分析理論と手法

	Safety-I	Safety-II
安全の定義	悪い方向へ向かう物事ができるだけ少ないこと	できるだけ多くのことが正しい方向へ向かうこと
安全管理の原則	何かが起こったときに反応し、応答する	事前対策的、発展や事象を予期するように努める
事故の説明	事故は失敗や機能不全が原因で起こる	結果によらず、物事は同じ方法で起こる
ヒューマンファクターの見方	責任	資源



IoT時代のセーフティ

システム障害や事故が発生した場合、原因は個々の構成要素の故障に留まらず、構成要素間や、
システムと人間との間の複雑な相互作用、さらには悪意を持ったサイバー攻撃に起因することがあり、原因究明が困難になりつつある。



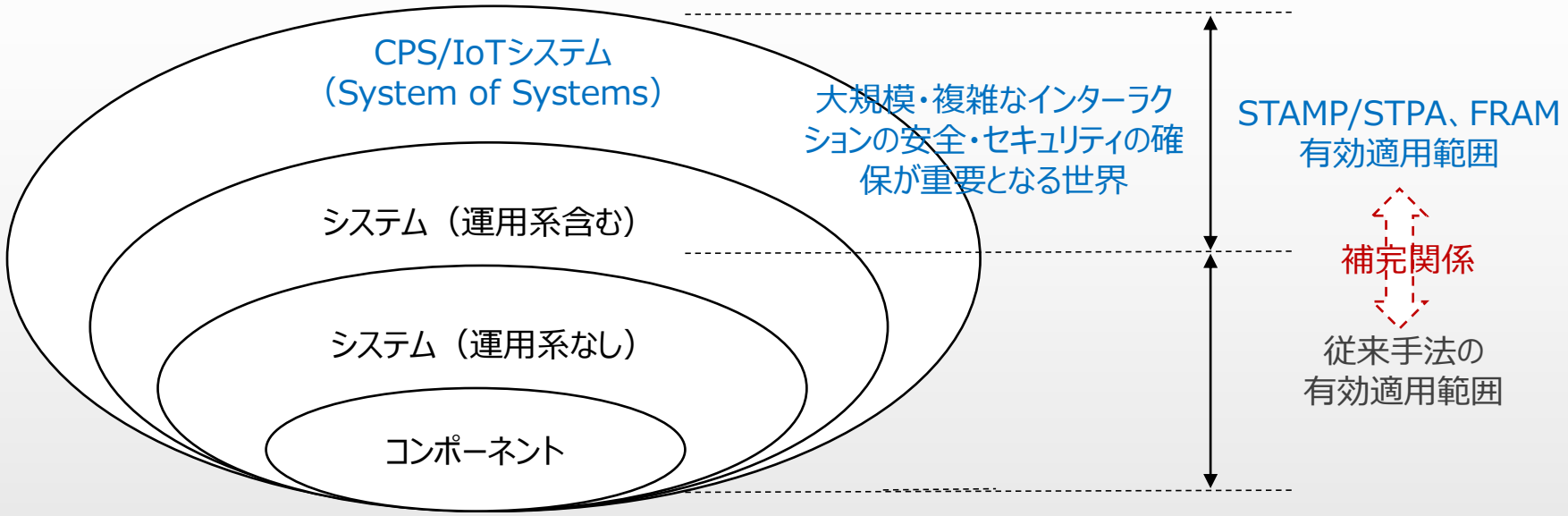
■セーフティ
偶発的なミス、故障などの悪意のない危険に対する安全を示す。

■セキュリティ
悪意をもって行われる脅威に対しての安全を示す。

今後、セーフティ＆セキュリティは同時に考えることが求められる

システム理論に基づいた事故分析手法の必要性

➢ セーフティ分析手法適用対象



従来の事故分析手法は、先入観や偏見による影響、偏りがある。
事故モデルはセーフティ分野の考え方なので、そのままセキュリティ分野への適用が難しい。

複雑なシステムを対象としたSTAMP、FRAMはセーフティを扱う理論。

IoTやAI、人間といった構成要素を含む複雑なシステム時代へむけて

**セーフティとセキュリティを垣根なく分析できる、
新たな事故分析手法が必要！！**

CASTとFRAMによる セキュリティ事故分析

～システム思考とレジリエンス～

STAMP/CASTとは

分析手順等の情報は
APPENDIXに記載してます

■STAMP/STPA

➢目的

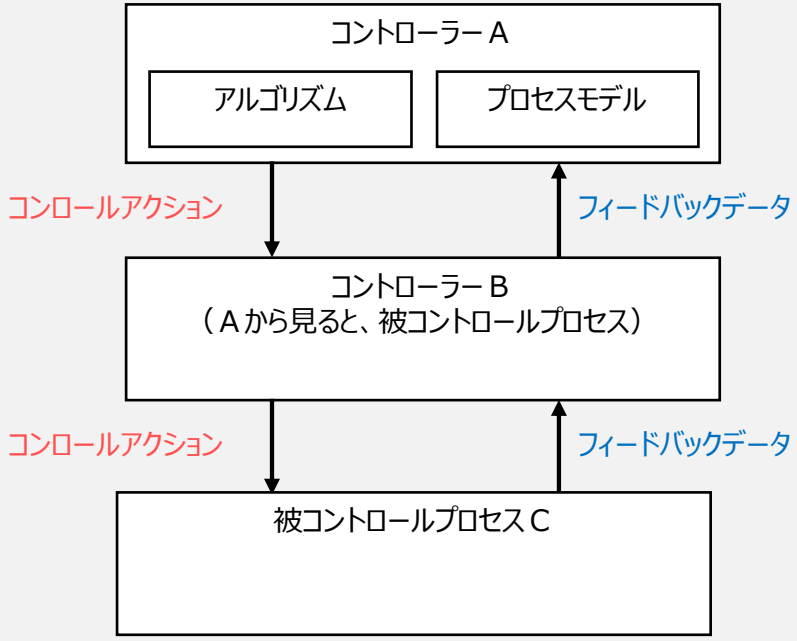
相互作用によって発生するハザードのリスクを分析する為（事前）

➢特徴

システムを安全に維持するための相互作用に着目して網羅的に確認することで想定外を削減

- ●コンポーネント間のインターラクション異常に着目する
- ●システムの大まかな構成要素が決まる概念設計の段階から適用できる

➢モデル図（コントロールストラクチャー図）



■STAMP/CAST

➢ 目的

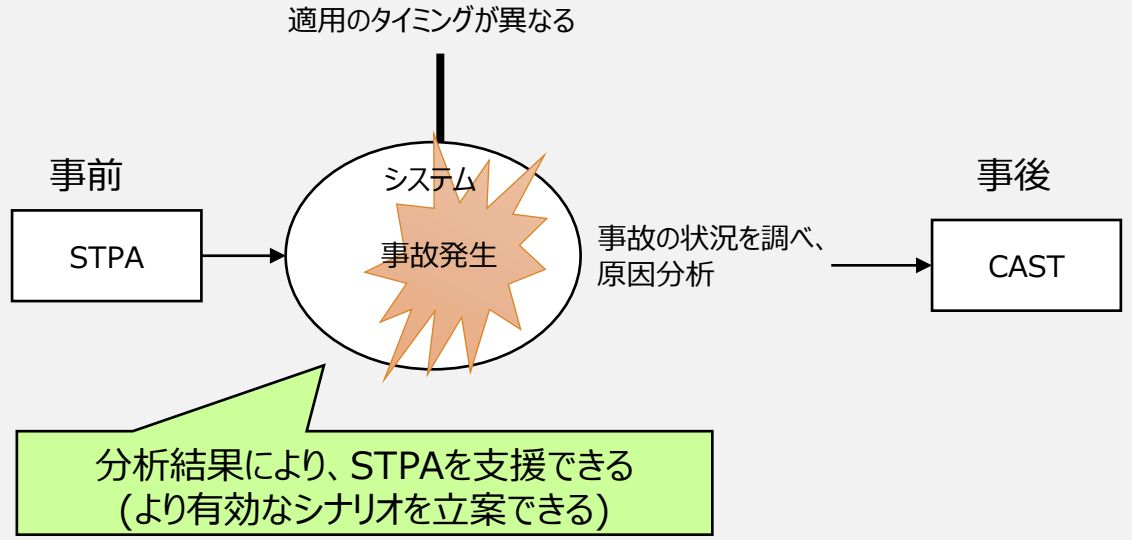
相互作用によって発生したハザードを分析する為

➢ 特徴

さらなる損失を防ぐ為に排除または管理する必要があるもっともらしいシナリオ（弱点）を識別できる

- ● 発生した特定のシナリオのみを識別できる
- ● 安全制御構造の破綻にフォーカスし、先入観や偏見による影響や偏りを小さくする（後知恵の偏り防止）

➢ STPAとCASTの違い



FRAMとは

分析手順等の情報は
APPENDIXに記載してます

- 目的

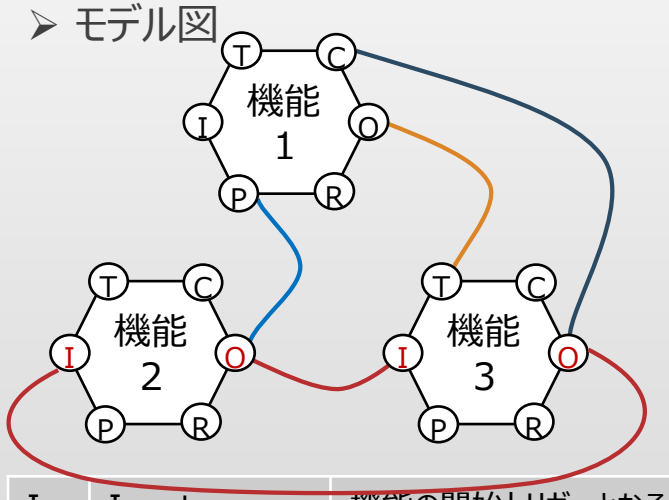
  システムの成功要因と、そこから導かれるリスク要因を発見する為

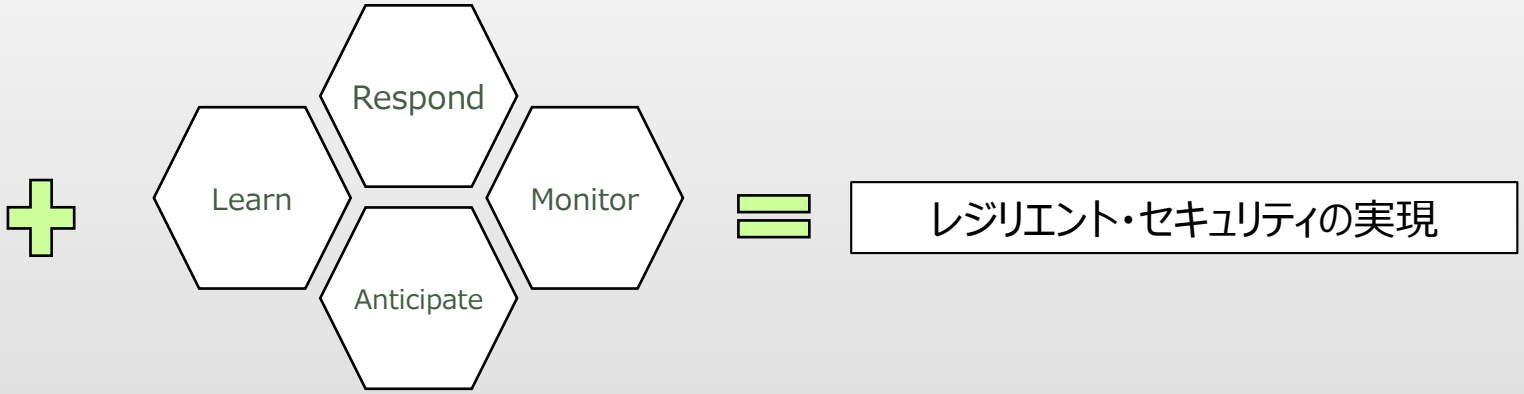
- 特徴

  機能と機能がどのように影響しあい、依存しあい、強めあい、弱めあっているのか（機能共鳴）を分析

  - 個別のコンポーネントやデータではなく、統合的な視点でネットワークトポロジーに着目する
  - システムの失敗要因を定義せず、成功要因に着目する

- モデル図



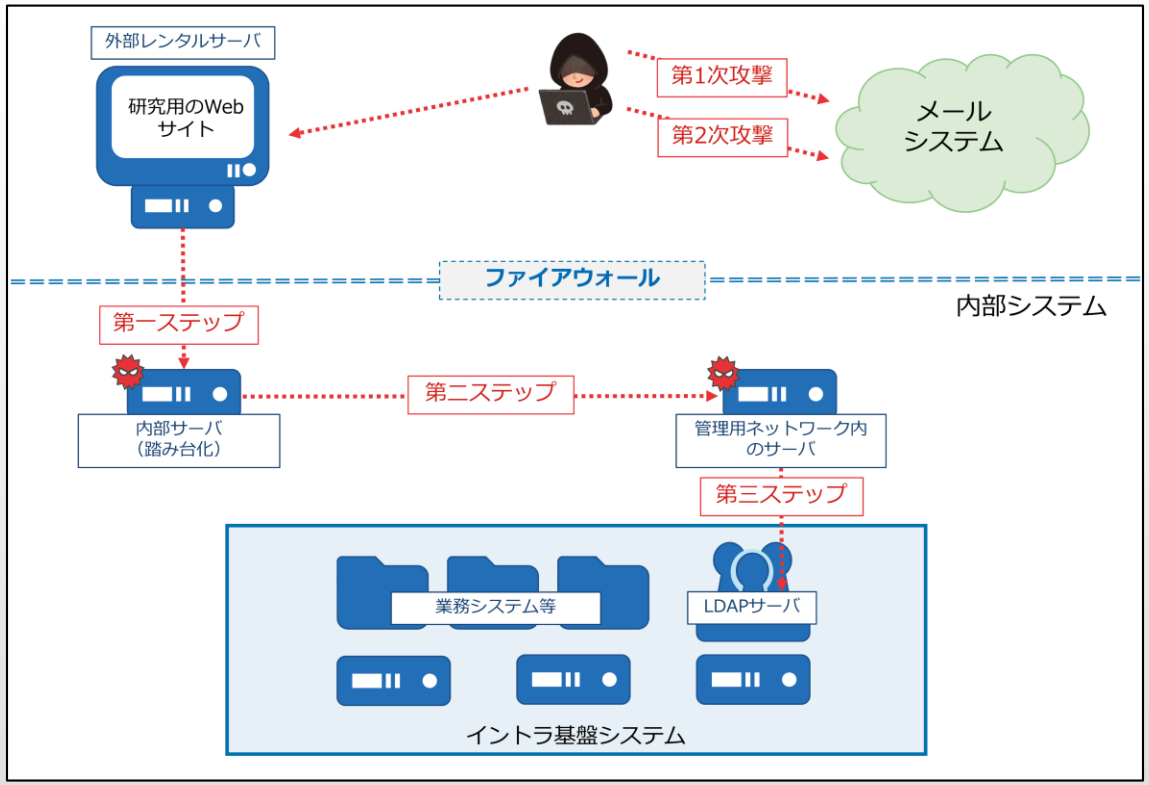


I	Input	機能の開始トリガーとなる入力
P	Precondition	機能の開始の前提条件となる入力
R	Resource	機能に実施に必要な資源となる入力
T	Time	機能の実施の制約となる時間情報
C	Control	機能の実施方法を変える制御入力
O	Output	機能の出力

Monitor	危険な予兆を察知する能力
Respond	予兆に素早く反応できる能力
Learn	過去の成功・失敗から学ぶ能力
Anticipate	将来のリスクを予測する能力

研究内容

2018年7月20に公開された「産総研の情報システムに対する不正なアクセスに関する報告」の事例を対象にそれぞれ分析。



セキュリティ・バイ・デザイン

STAMP/CAST：システム理論

システムや機能間の相互作用に着目してシステム全体への事故要因を分析

Monitor、Respond、Learn、Anticipate
のコア能力によって、サバイバルな環境に順応する

FRAM：レジリエンス・エンジニアリング

予め失敗事象を定義せず、
各機能の関係性及び相互の入出力の変動に着目した分析

出典：産総研の情報システムに対する不正なアクセスに関する報告（国立研究開発法人 産業技術総合研究所）

セーフティの分析手法を用いて、セキュリティ分析に適用できるか研究

STAMP/CAST

分析の目的

セキュリティの従来分析（報告書の結論）とは違う観点で問題点を抽出し分析を行うことで、
報告内容だけでは見えていない問題を抽出できるのかを検証する。

分析結果からの考察

報告内容だけでは見えてこない 背後要因に関する問題 や システム上の 具体的な対応策を抽出できた。

- 非安全なCAとコンテキスト要因を「同時に分析」し、問題の直接原因と発生させる背後要因を抽出できる「手順」が効果的。
- マネジメント面は、強化、見直し等の曖昧な表現になりやすいが、システムミック要因分析が具体策を出すのに有効。
  例えば、マイスター認定制度導入によるスキルアップなど。

適用する場合への提言

以下を行うことで未然防止の分析に繋げることができる。

- 抽象化されたCS図の標準パターン化とそれぞれにCS図に紐づいた事例集の蓄積
- STPAを参考に、STPA/CASTで共用できるガイドワード、ヒントワードの定義

FRAM

分析の目的

事故内容の説明及び対策案を創出するために、適用可能か検証する。

分析結果からの考察

弱点を克服するだけでなく、 強固な対策案を実現できた。適用可能である。

- FRAMのモデル上で接続数の多い2機能に着目。その機能周りのクリティカルパスから弱点に着目したことで創出。
- Monitor、Learnの観点を追加することで、セキュリティが強靭となる機能追加が可能。

適用する場合への提言

- FRAM分析において、 各機能間での接続数の密度やクリティカルパス、 相互作用を意味するループ構造に着目できる特徴がある。

情報システムに その特徴を適用した場合、

- システムを俯瞰的に見ることができ、前述の構造的特徴に着目することで、対策をより深く考えることができる。

的なシステムは、基本的に入出力が一方通行になるように設計されていることが多いため、活用難度は高い。

各分析手法の比較

被害を発生・拡大させた要因		産総研	CAST	FRAM
① システム・機器の問題	メールシステムのログイン方法	○	◎	◎
	内部サーバと連携していた外部サイト	○	◎	○
	広域でフラットな内部ネットワーク	○	○	○
	内部ネットワークの不十分な監視	○	○	◎
	アクセス制限のなかった管理用ネットワークのサーバの存在	○	◎	◎
	情報機器の脆弱性	○	○	×
② パスワード・暗号鍵の管理と強度の問題		○	◎	×
③ 外部委託業者の管理の問題		○	○	×
④ マネジメントの課題		○	◎	×

◎は報告書の結果に対して要因を多く抽出できたもの
×は要因を抽出できなかったもの

STAMP/CAST：トップダウン

報告書で抽出されていた要因は全て抽出。中でも特に弱点であったと考えられる要因の特定に成功。

FRAM：ボトムアップ

強化することでセキュリティが強靭になる要因の特定に成功。

研究成果のまとめ

STAMP/CASTを用いて、トップダウンで俯瞰的/網羅的に分析可能。

着目すべき機能を中心にスコープを絞った後、
FRAMを用いて、別の視点から分析を加えることでレジリエントな対策が立案可能。

- STAMP/CASTとFRAMで分析結果の情報量に大きな差があり、CASTでの分析結果の情報量はFRAMよりはるかに多い。
- STAMP/CASTでの分析は俯瞰的/網羅的に分析でき、膨大な量の情報が結果として得られている。
- FRAMは主要な機能を着眼点として決めてモデル化し、４つの機能を追加することで新たな視点でのレジリエントな対策を追加できる。

セキュリティ(事故)分析に、
セーフティ分析手法のSTAMP/CASTとFRAMは活用できる。

今後の課題と対策案

- ✓ CASTでは、時系列的な分析方法が言及されておらず、経時的な変化に対する欠陥を洗い出せなかった。
  ⇒イベントツリーなどの時系列事象を正確に把握する別手法の併用を検討。

- ✓ FRAMでは、明確な手順が存在しておらず試行錯誤や創意工夫により実施する部分が多くあった。
  分析過程の事象のモデル化においては三者三様のモデルが出来上がり、個人差が大きく発生していた。
  ⇒分析事例を増やし、分析手法のノウハウを蓄積し、手順の標準化や分析のガイドラインの整備を検討。

⇩ トップダウンのCAST、ボトムアップのFRAMの分析手法であり、分析過程も大きくことなる

- ✓ 双方の手法を融合し、トップダウン/ボトムアップの分析を同時に実施できる手法の確立。
- ✓ 分析対象の特徴からより適正のある手法を選択する判断基準を確立。

⇩ 例えば

- ✓ CASTを用いてトップダウンで俯瞰的/網羅的に分析し、着目すべき機能を抽出。
- ✓ 抽出された機能を中心にスコープを絞って、FRAMを用いて別の視点から分析を加え、
  レジリエントな対策を立案する方法。

第８分科会 演習コースⅢ セーフティ・セキュリティコース

１年間ありがとうございました！！

主査

- 金子 朋子（情報セキュリティ大学院大学）

副主査

- 髙橋 雄志（アイダック）

アドバイザー

- 佐々木良一（東京電機大学）

研究員

- 三宅 保太朗（DTSインサイト）
- 大西 智久（NTT ｺﾐｭﾆｹｰｼｮﾝｽﾞ）
- 壁谷 勇磨（日立製作所）
- 中嶋 良秀（ノーリツ）
- 藤原 真哉 （NTT ｺﾐｭﾆｹｰｼｮﾝｽﾞ）
- 山口 賢人（TIS）
- 須藤 智子（日立ソリューションズ）
- 出原 進一（パナソニック）
- 金沢 昇（ﾃｯｸｽｴﾝｼﾞｿﾘｭｰｼｮﾝｽﾞ）
- 西 啓行 （富士通）
- 山崎 真一（富士ゼロックス）

※順不同

発表日に受けたQA

Q1. 論文で見て欲しいポイントを教えてください。

全てがお勧めですが、4.3の考察とそれに付随する付録に、我々が得た知見や所感が書かれています。共通のトピックや悩みなどがあれば参考にしてください。新たな試みなので類似資料は少ないといえます。

Q2. セキュリティにフォーカスしているが、セーフティについても見えたこと等ありますか？

今回の事例はセーフティ要因が見えてこない（あてはまらない）のでセーフティ要因が引き金となった事故ではないことが証明されました。（例えば、攻撃者によるアタックではなく、機器が正しく機能していないための事故であったなど）
偶発的な要因が主であれば、セーフティの事故といえるかもしれません。

Q3. 某決済システムのセキュリティ問題のように、経営の要因まで含めて適用できますか？

CS図から見えるUCA、FRAM図におけるウィークポイント（ストロングポイントの裏返し）の要因として定義することで可能になると考えます。

Q4. 最近の事故で、HDD転売というのがあったかそういった事故の分析は可能か？

CS図やFRAM図でモデルを表すことができれば可能であると考えます。
ただし、どちらもモデル化するのには深い理解が必要です。
例えば、CS図では制御を指示と置き換えて、指示系統と命令実行にエラーが発生すると考えることでモデル化できるものと思われます。

STAMP/STPA

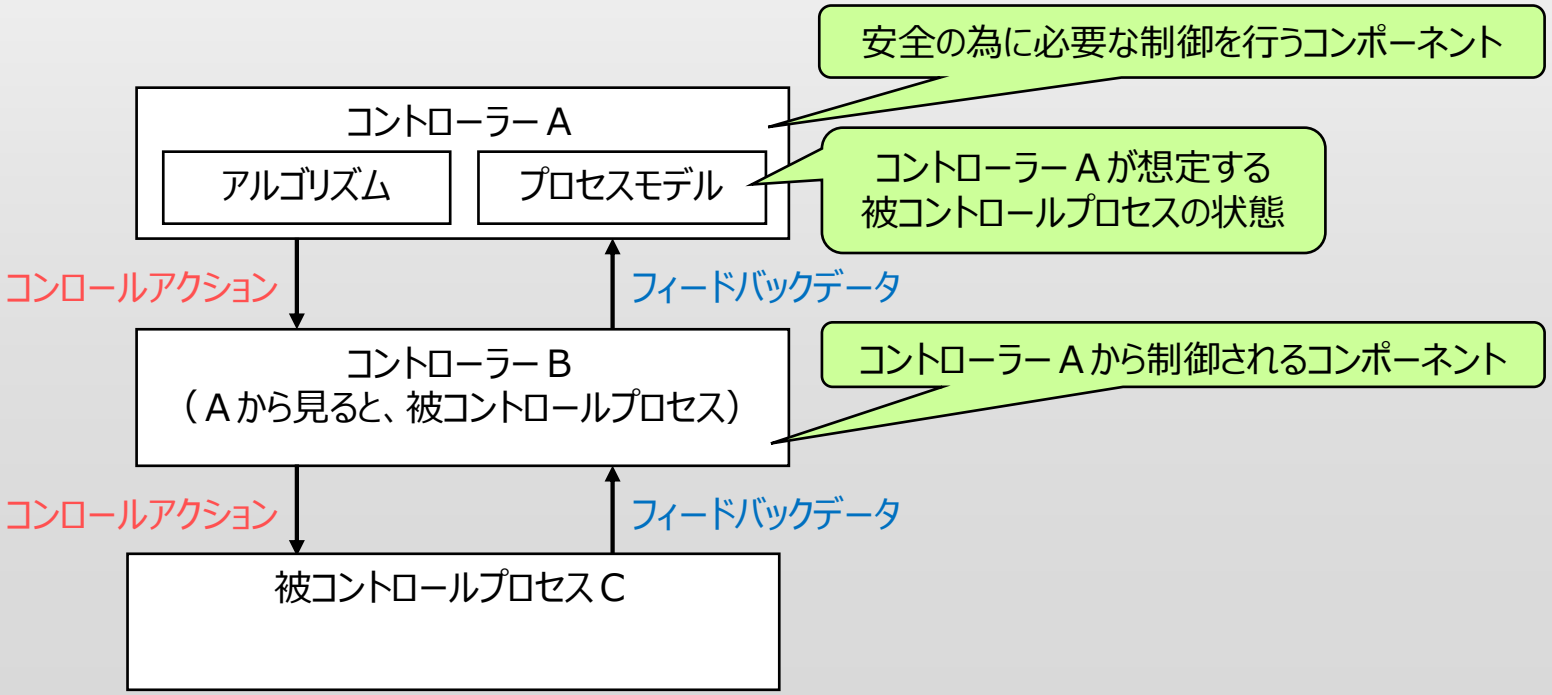
APPENDIX-A1

STAMP/STPA（Systems-Theoretic Accident Model and Processes）

➢目的
相互作用によって発生するハザードのリスクを分析する為（事前）

➢特徴
システムを安全に維持するための相互作用に着目して網羅的に確認することで想定外を削減
- コンポーネント間のインターラクション異常に着目する
- システムの大まかな構成要素が決まる概念設計の段階から適用できる

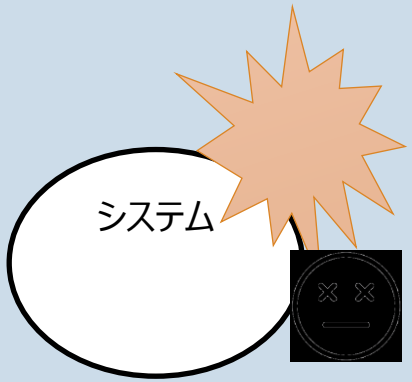
➢モデル図（コントロールストラクチャー図）



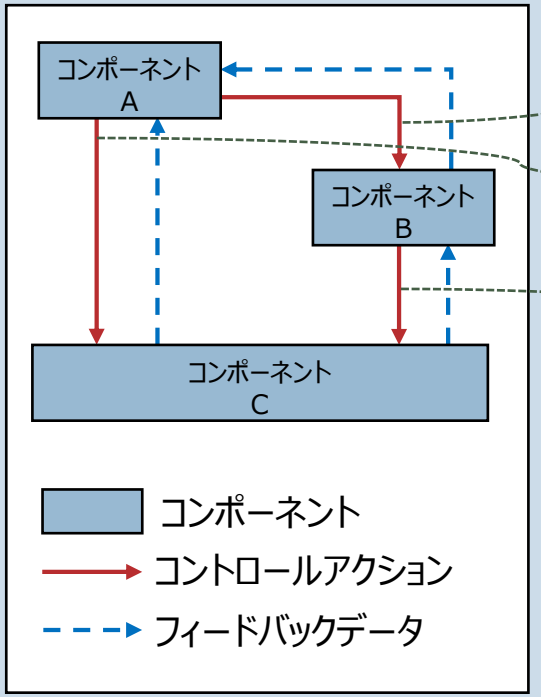
STAMP/STPA分析手順

【Step0-準備1】 ⇨ 【Step0-準備2】 ⇨ 【Step1】 ⇨ 【Step2】

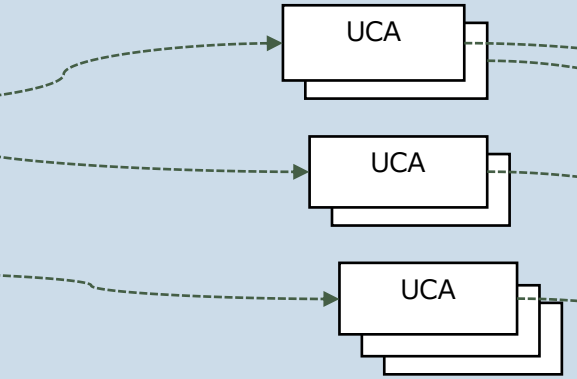
システムレベルのアクシデント、ハーザード、安全制約の識別



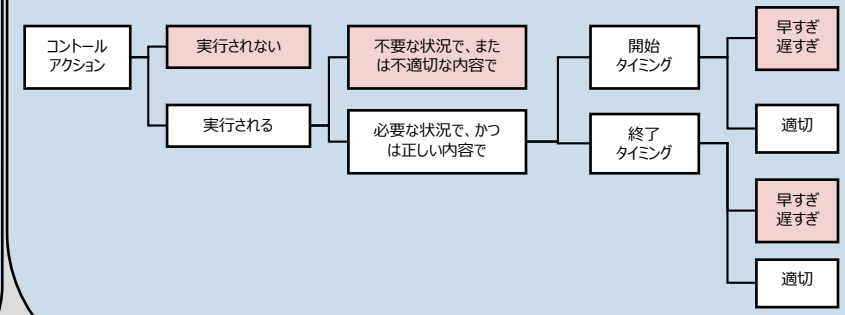
コンポーネント間の制御関係を表すモデルの構築
※コントロールストラクチャー



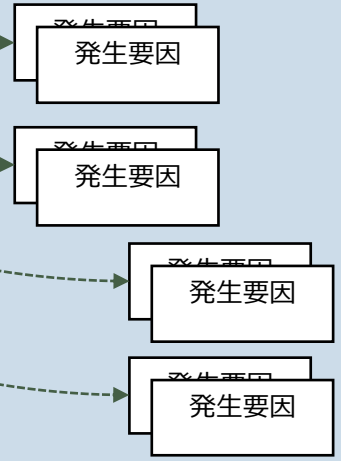
ハザードにつながるコントロールアクションの識別
※UCA（Unsafe Control Action）



危険な制御のパターンを利用して分析



UCAの発生要因分析
※HCF（Hazard Causal Factor）



コンポーネントが満たすべき安全要件を導出

詳細は、「はじめてのSTAMP/STPA」を参照。https://www.ipa.go.jp/files/000055009.pdf

STAMP/CAST

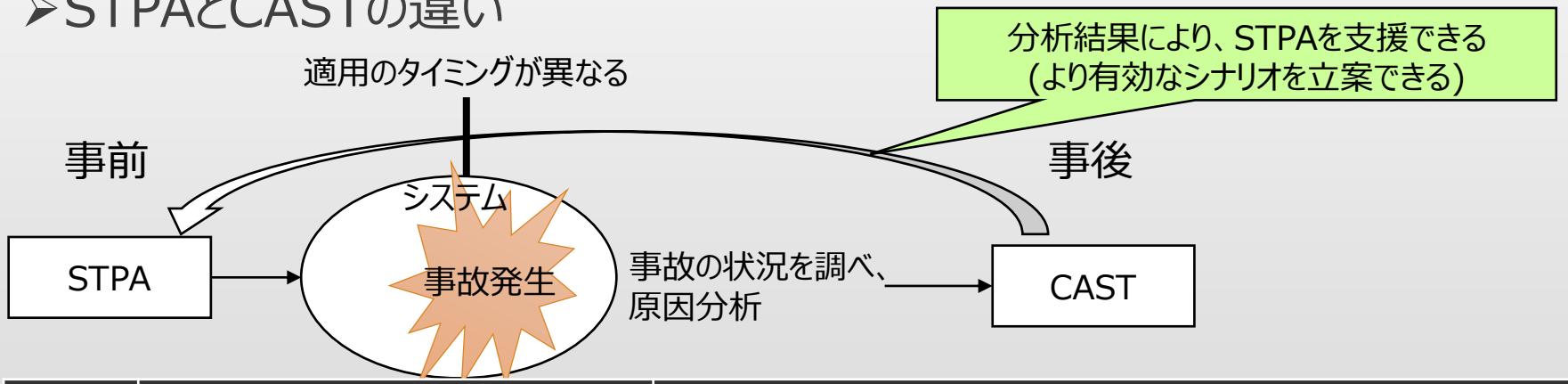
APPENDIX-A2

STAMP/CAST（Causal Analysis using System Theory）

➢目的
相互作用によって発生したハザードを分析する為（事後）

➢特徴
さらなる損失を防ぐ為に排除または管理する必要があるもっともらしいシナリオ（弱点）を識別できる
- 発生した特定のシナリオのみを識別できる
- 安全制御構造の破綻にフォーカスし、先入観や偏見による影響や偏りを小さくする（後知恵の偏り防止）

➢STPAとCASTの違い



手法	作成するシナリオ	期待効果
STPA	潜在的なシナリオ	設計が作成される前に使用できる為、 セーフティ&セキュリティに関する開発コスト低減が可能
CAST	発生した特定のシナリオ	更なる損失を防ぐ為に、排除、管理する必要があるプロセスを特定することで、 STPAプロセスを支援可能。

STAMP/CAST分析手順

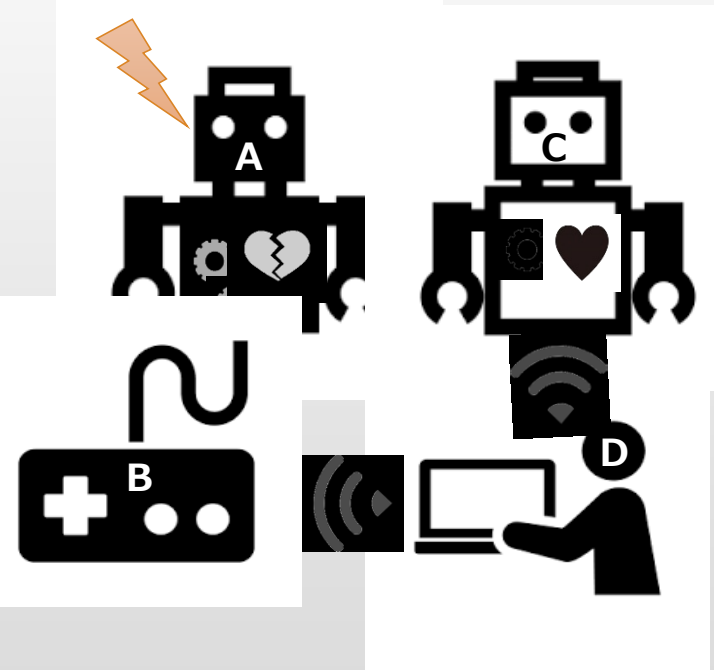
1．不具合、事故情報の内容把握

① 損失に関与したシステムと分析対象の範囲を定義

② 識別したハザードからハザードを防止するために必要なシステムレベルの安全制約を特定

③ 損失につながるイベントチェーンを究明

STAMP/STPAと同じ



アクシデント	ハザード	安全制約
システムAの機器１の異常に対して、システムA内で対処できず、物理的に離れた組織Dで対処せざるを得ない事象が発生	システムA内の機器異常にシステムA自ら対処できない	システムA内の機器異常にシステムAが自動で対処すること

損失に近接する発生イベント（What?：何が起きたのか）	イベントが発生した理由の回答を求める質問を作成（Why？：原因究明の為明らかにしたいこと）
機器3が異常を検知しなかった	何故、異常を検知できなかったか？
	何故、応答が一定期間内場合を設計しなかったのか？
	何故、異常を正常とみなしたのか？
	・・・

STAMP/CAST分析手順

2. 対象のシステム分析

① 重要なイベント(障害および安全でない相互作用)とこれらのイベントから生じる質問を特定して、物理的な設計の欠陥と状況要因を説明する

実際に損失があったコンポーネント単位で、以下の観点から分析

この事故の防止のためのすべての物理的な安全要件と制約を識別
物理的な装置のあらゆる故障もしくは不適切な制御を識別
物理的な故障もしくは不適切な制御を説明するコンテキスト要因を識別

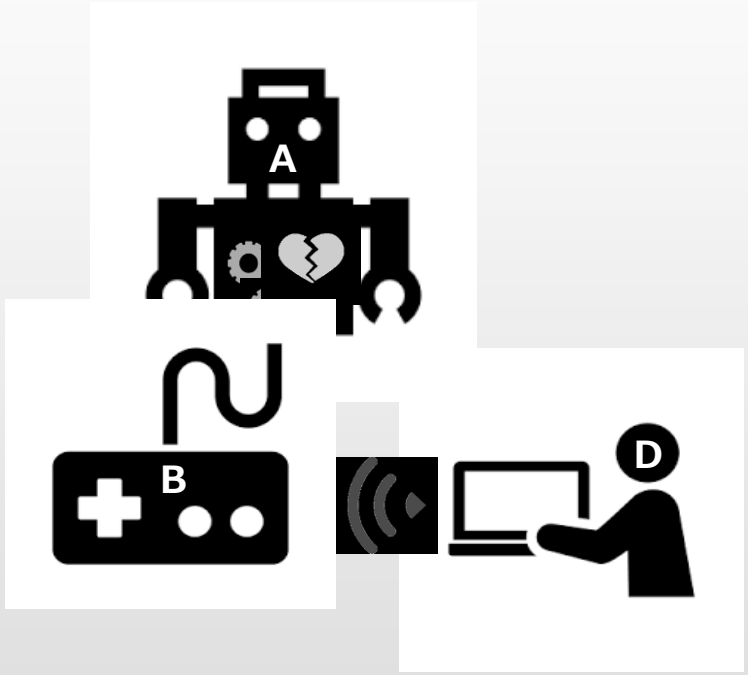
損失に関連するコンポーネント	安全上の責務	非安全なコントロールアクション	プロセス/メンタルモデルの欠陥	意思決定された状況・背景
機器3	機器2のステータスを監視し、異常が返ってきたら機器2に切替コマンドを発行する	異常が返ってきたのに、機器2に切替コマンドを発行しなかった	機器3の切替コマンド発行が無効になっていることを検知できない	数日前に、メンテナンス対応のため切替コマンド発行を無効にする設定にした後、そのままになっていた

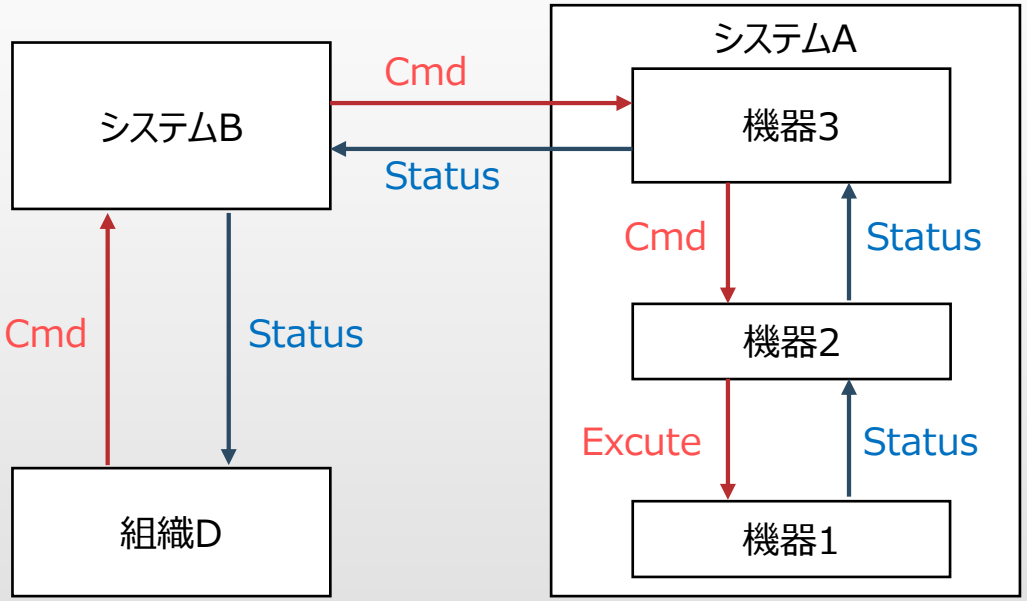
STAMP/CAST分析手順

STAMP/STPAと同じ

3. 安全コントロールストラクチャの作成

① システムの構成要素間の構造と相互作用を表すために、既存の安全制御構造をモデル化する





STAMP/CAST分析手順

4. 論理モデルの分析

① 安全コントロールストラクチャで損失があったコンポーネントとその周辺のコンポーネントを抽象的事象と捉え、なぜ不適切な制御に寄与したかを解明

以下の観点から分析

抽象化レベルの制御に対する、安全制約の責務を識別
非安全な決定と制御アクションを識別
非安全な決定と制御アクションを説明するプロセスモデルの欠点を識別
その時点でなぜその振る舞いが適切に思えたか説明するコンテキスト要因を識別

損失に関連するコンポーネント	安全上の責務	非安全なコントロールアクション	プロセス/メンタルモデルの欠陥	意思決定された状況・背景
機器3’	対象機器の状態を監視し、返ってくるステータスに応じてコマンドを発行する	ステータスに応じたコマンドを発行しない	コマンド発行を制御するための設定値が、通常運用時と異なっていることを検知しない	機器設定値の確認は変更者の責務とし別途運用ルールを定めていたため、システム的に検知する手段を備えていなかった

STAMP/CAST分析手順

5. 制御構造の欠陥特定

① 損失の原因となったシステミック要因を調査することで制御構造全体の欠陥を特定する。
システム全体を俯瞰し、手順2から4の結果から個々のコンポーネントが個々の安全責任を果たせなかった理由、コンポーネントの動作が一緒になってシステムの安全制約を満たせなかった理由を抽出

↓ 抽出後、システミック要因（経時的な変化とダイナミクス）に分類

情報交換と相互連携
安全な情報システム
安全なマネジメントシステムの設計
安全な文化

② 経時変化により劣化し事故に至る要因となった制御構造全体の欠陥を特定する。
手順2から4で抽出した欠陥から、システミック要因に当てはまる欠陥があるか確認する 。

情報交換と相互連携	安全な情報システム	安全なマネジメントシステムの設計	安全な文化	経時的な変化とダイナミクス
機器の設定を通常運用から変える際の運用ルールが周知できていなかった	設定値変更時の作業記録及び通常運用時の設定値の正当性を照合する機能がなかった	機器設定を変えた後に元に戻すことの確認をとるプロセスがなかった	メンテナンス作業が運用に与える影響を精査せずに作業する風土があった	当初は厳格なルールで運用していたが、作業効率の低下を招くため、現場作業者の判断で逸脱する状況になっていた

STAMP/CAST分析手順

6. 改善勧告（案）の作成

① 将来同様の損失を防ぐために、統制構造の変更に関する推奨事項を作成。
機器やオペレータ、さらに組織といった要素から成るコントロールストラクチャを、
どう変えると欠陥を防止できるか提言する。

欠陥	改善勧告（案）
自身の状態が異常であることを検知しない	通常運用とかけ離れた機器状態が続く場合はアラートを出す仕組みを入れる
機器の設定を通常運用から変える際の運用ルールが周知できていなかった	メンテナンス等で機器設定を変える際の作業/運用ルールを運用チームで教育する
機器設定変更の作業記録を残すデータベースがなかった	機器設定変更の作業記録データベースを用意し、運用チームで共有する
・・・	・・・

FRAM

APPENDIX-B

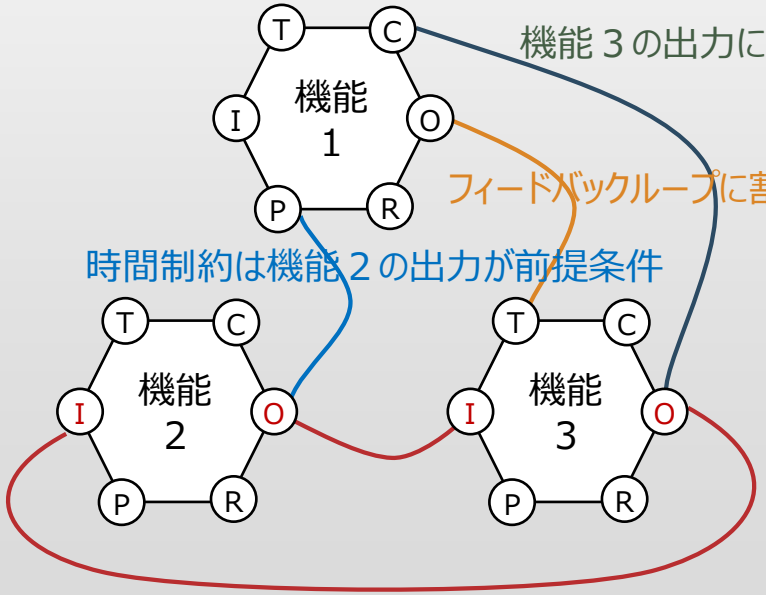
FRAM

➢目的
システムの成功要因と、そこから導かれるリスク要因を発見する為

➢特徴
機能と機能がどのように影響しあい、依存しあい、強めあい、弱めあっているのか（機能共鳴）を分析
- 個別のコンポーネントやデータではなく、統合的な視点でネットワークトポロジーに着目する
- システムの失敗要因を定義せず、成功要因に着目する

事故は故障やミスから起こらないというのが最近のトレンド

➢モデル図



I	Input	機能の開始トリガーとなる入力
P	Precondition	機能の開始の前提条件となる入力
R	Resource	機能に実施に必要な資源となる入力
T	Time	機能の実施の制約となる時間情報
C	Control	機能の実施方法を変える制御入力
O	Output	機能の出力

機能 1， 2， 3 でダイナミックな共鳴関係が築かれている
不意なタイミングで機能 3 が処理時間超過となるリスクがあることを読み取れる

FRAMの分析手順

1. モデリング手順

① 質問による機能の把握

機能の６要素を網羅的に分析する。
この網羅性によって、機能間の相互作用の見落としがないことが保証される。

	その機能の目的は何か？
	機能はどのような処理を行っているか？
	機能にはどのような入出力が存在するか？

機能概要が把握できたら、詳細を把握する

I	その機能の開始トリガー（入力）は何か？
	条件が変わった場合、どのように適応するか？
	正常でない条件にどう反応するか？
R	リソースは安定的に供給されるか？不安定要因は？
	外部環境はどのくらい安定？不安定要因は？
	正常でない条件はたびたび発生？
P	「当然」と思われている前提条件はあるか？
T	時間制約によるプレッシャーはどこにかかるか？
	特別なスキル，特別な高機能，特別な高信頼性を必要とする個所は？
C	最適な実行方法というものが存在しているか？

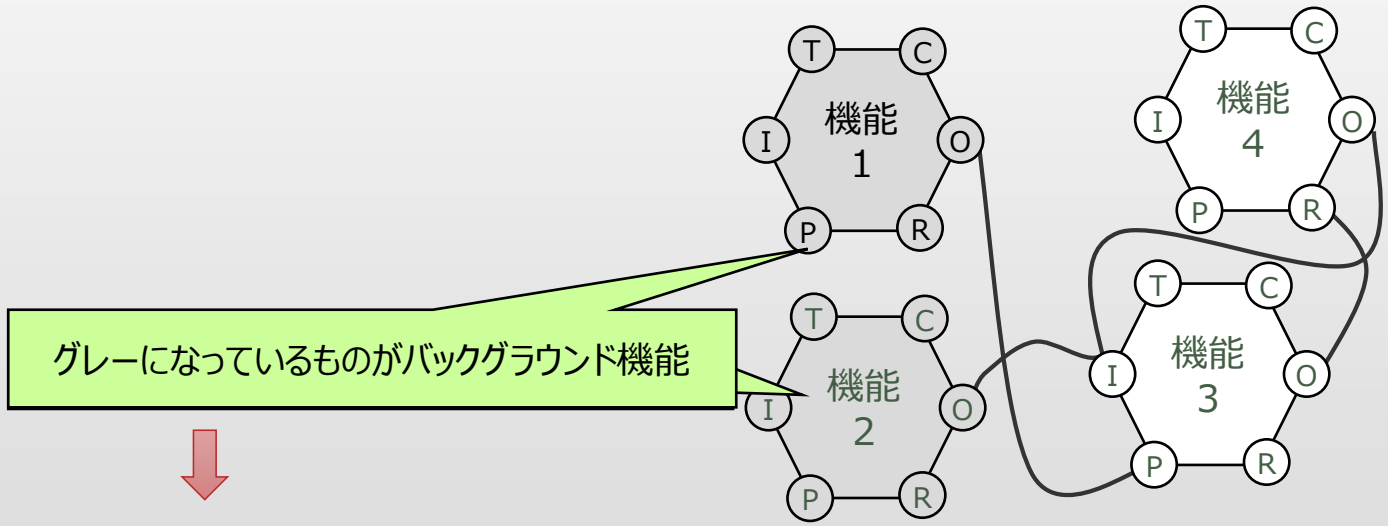
FRAMの分析手順

② 各機能の定義

各要素の名前（やりとりされる情報・データ・もの・締め切り時間）
相手の機能の名前

③ モデルの可視化

FRAM Visualizerで行う。(http://functionalresonance.com/FMV/index.html)



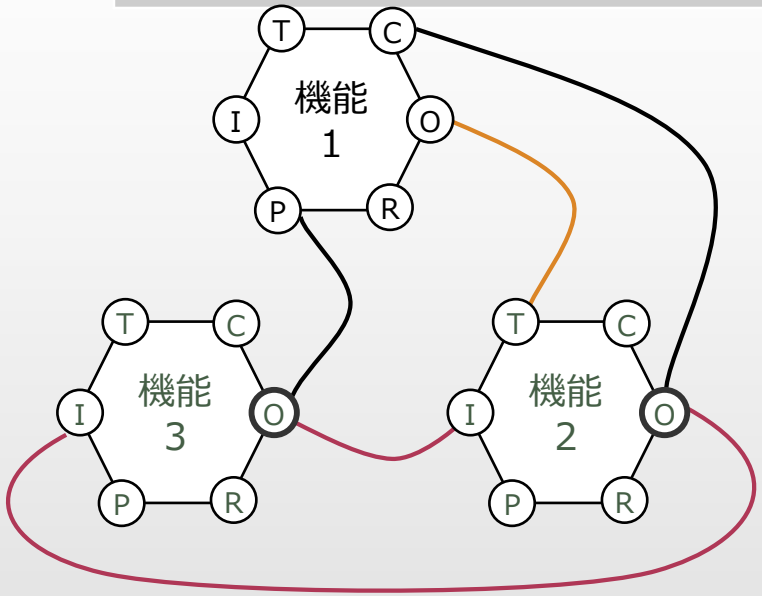
モデルの外縁に該当し、
注目する機能からバックグラウンド機能までがFRAM分析の対象となる

FRAMの分析手順

④ 可視化したモデルを使った分析

このシステム（モデル化した範囲全体）の成功要因は何か？

成功要因を識別し、それを育てると共に、成功要因の実現を阻むリスクを抽出する為、必ず先に成功要因を分析すること



機能2や機能３からの放射線状の出力

機能3と機能2の間のループ構造

機能1と機能2の間のループ構造

機能3から機能2・機能1を経由して機能3に帰る大ループ構造

機能3と機能2は通常はシーケンシャルに処理を行っており、
機能1からの時間制約が発生しても、機能3、2の処理順序逆転することがない。
（必ず順番が守られる）
これが成功要因の1つ。

このシステムのリスク要因は何か？

機能2は時間制約あり。制約を満たせない場合、ストップする

機能2の停止により、機能3は開始トリガーを失う

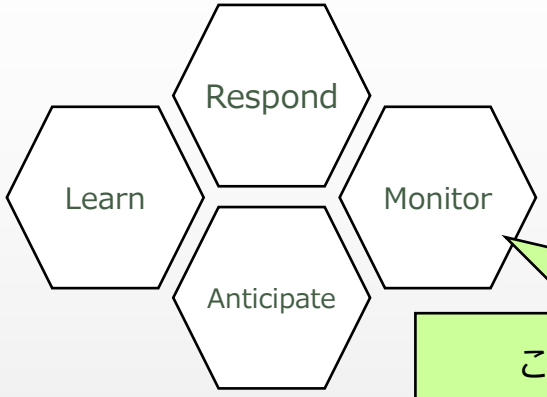
機能3がタイムアウトを検知して再実行するとしたら、その時の機能2はどのような状態か？機能2が停止している状況で動作できるのか？

成功要因の分析からリスク要因の分析につなげることが重要

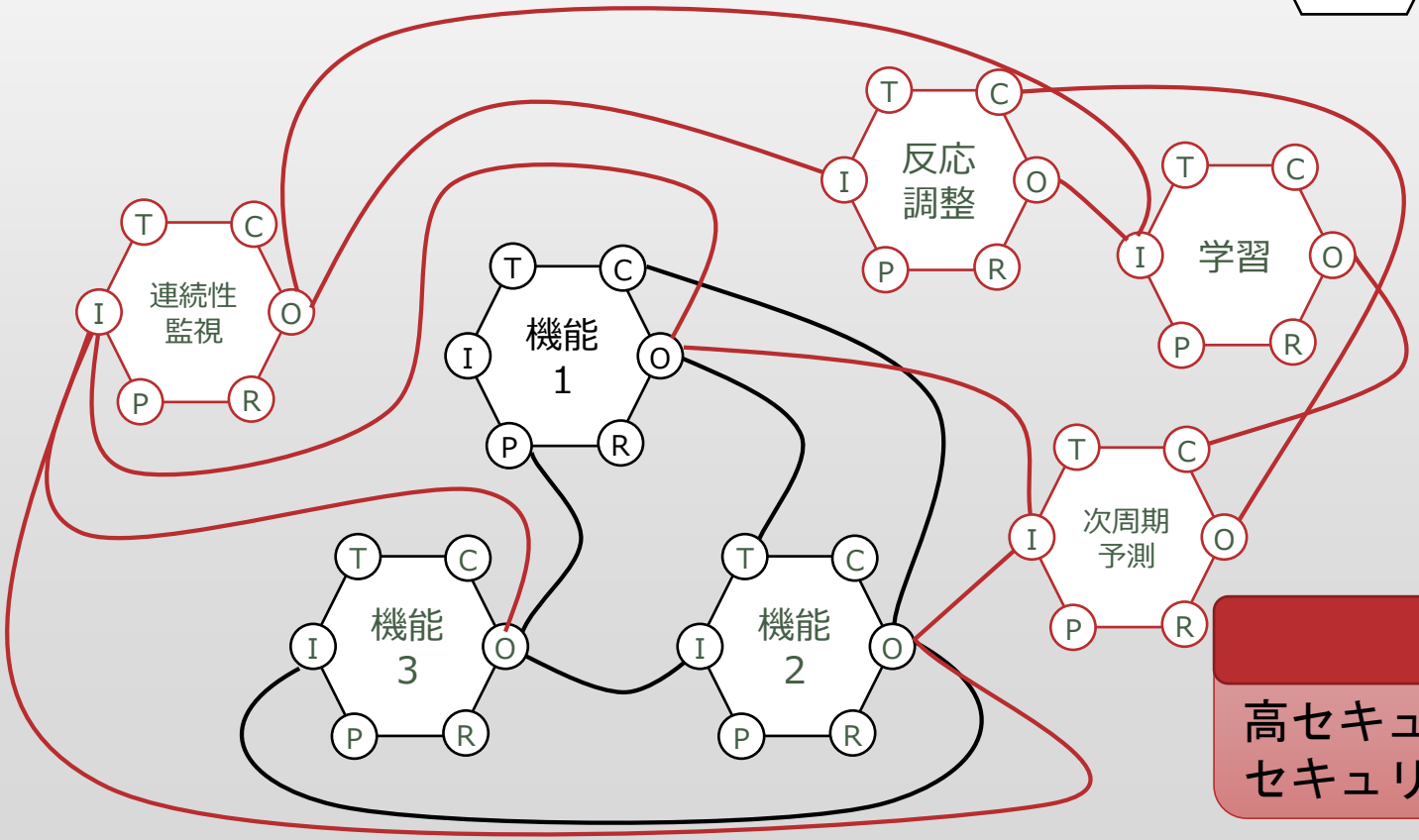
FRAMの分析手順

2. レジリエンス機能の追加

Monitor	危険な予兆を察知する能力
Respond	予兆に素早く反応できる能力
Learn	過去の成功・失敗から学ぶ能力
Anticipate	将来のリスクを予測する能力



この4機能により、乗っ取りに対してきわめて強靭になる



レジリエント・セキュリティの実現

高セキュリティ＝ 高パフォーマンス
セキュリティとパフォーマンスのトレードオフからの脱却