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～

株式会社　DTSインサイト
第二事業本部　第三システム事業部　開発課
三宅 保太朗
E-mail：Yasutaro.Miyake@dts-insight.co.jp

共同著者
○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）

※順不同

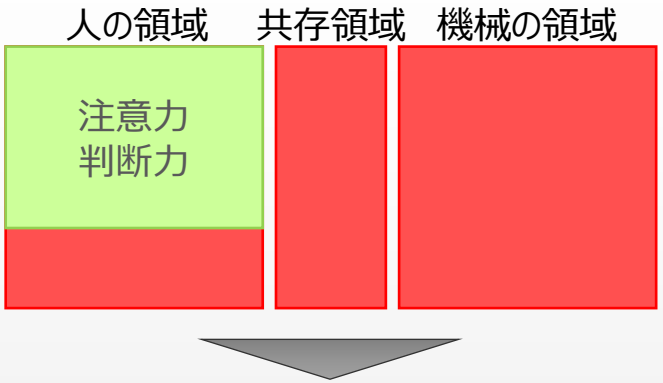
須藤 智子（日立ソリューションズ）
出原 進一（パナソニック）
金沢 昇（ﾃｯｸｽｴﾝｼﾞｿﾘｭｰｼｮﾝｽﾞ）
西 啓行　（富士通）
山崎 真一（富士ゼロックス）
金子 朋子（情報セキュリティ大学院大学）
髙橋 雄志（情報セキュリティ大学院大）
佐々木 良一（東京電機大学）

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

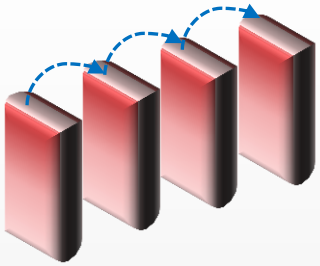
・人と機械の共存を可能に

・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を活用し、人間と機械が協調して安全を確保する時代が到来

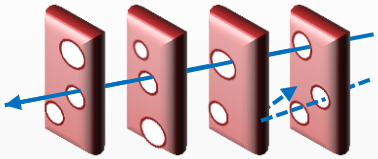
従来の事故モデルと安全分析手法

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)

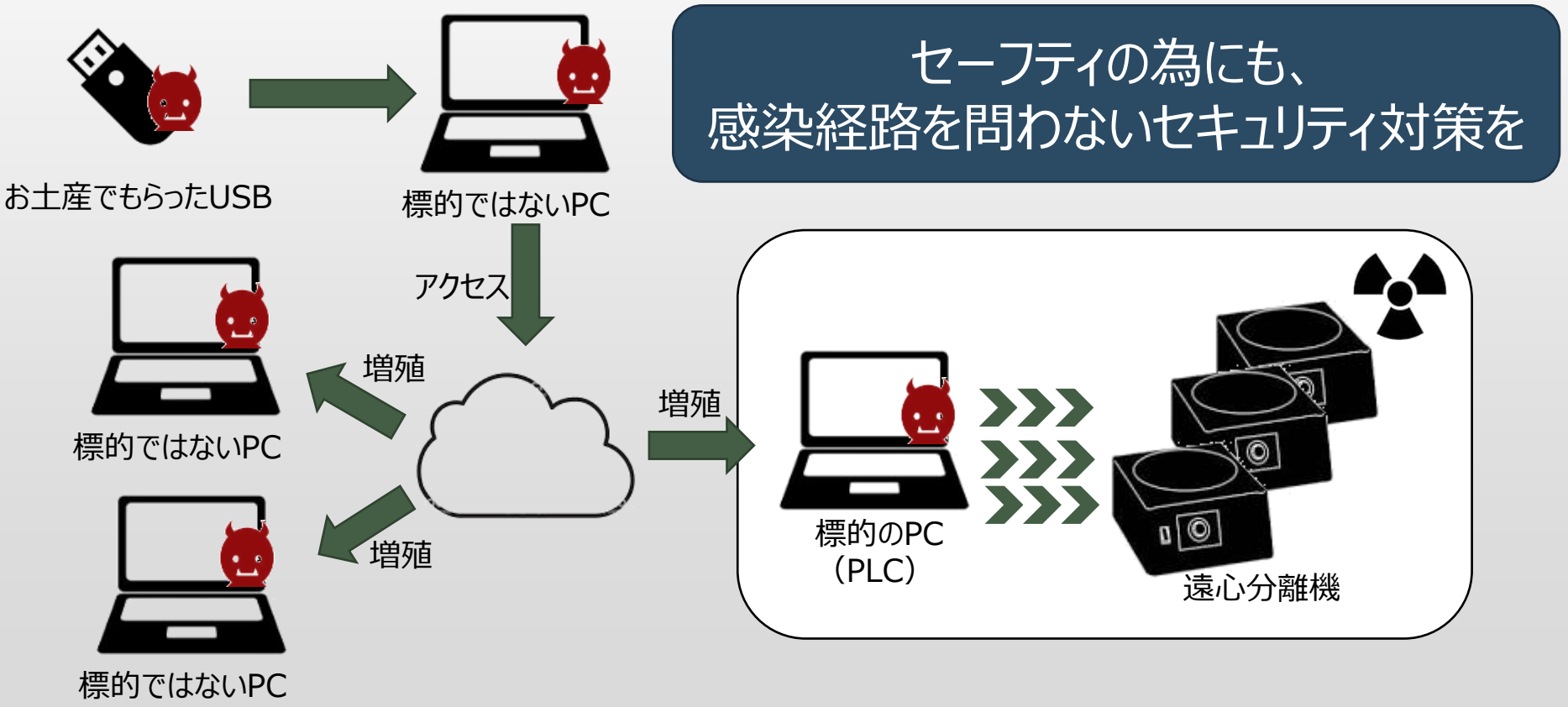
FMEAやFTAの中でガイドワードの考え方を用いる

※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）

新たな事故モデルの具体例

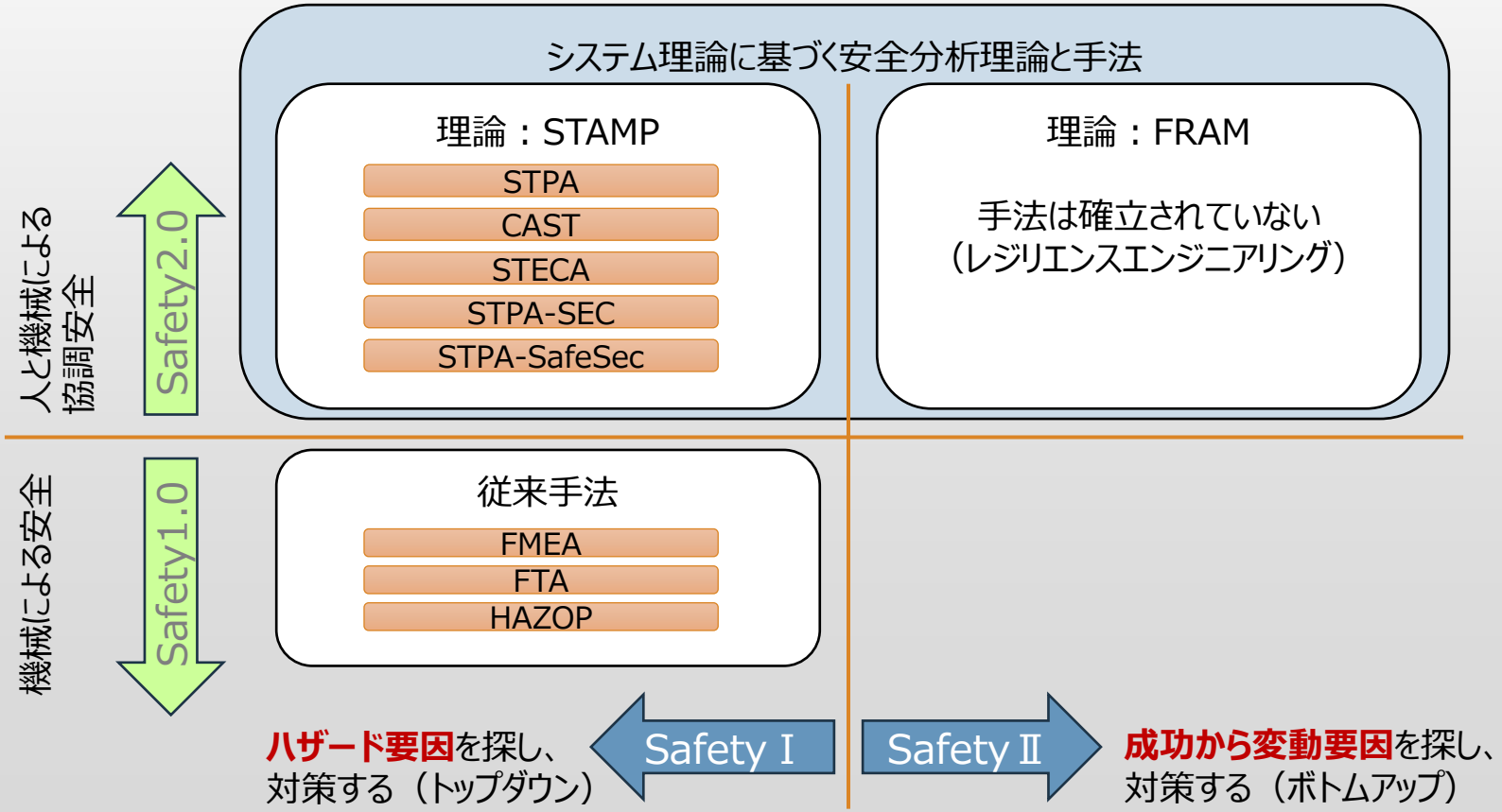
Stuxnet（スタックスネット）。2010年6月にベラルーシ共和国で発見。
2010年9月にイランの核燃料施設のウラン濃縮用遠心分離機を標的に、
PLCを乗っ取り、周波数変換装置が攻撃。約8400台が破壊された。



セーフティの為にも、
感染経路を問わないセキュリティ対策を

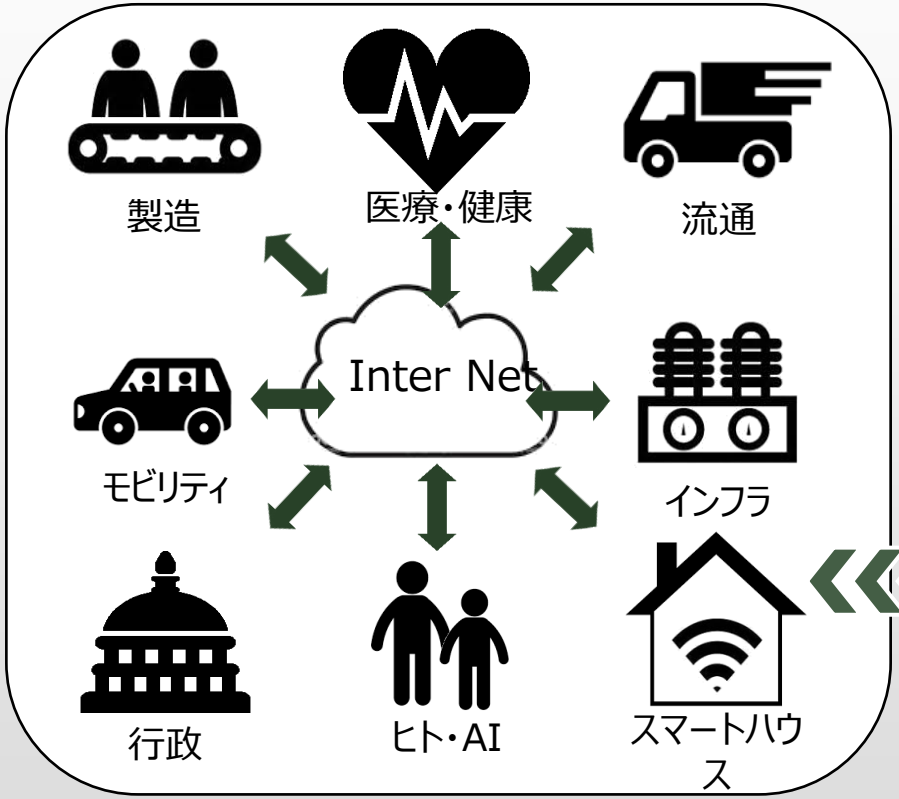
Safety-Ⅰ,Ⅱとセーフティ分析理論と手法

	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。



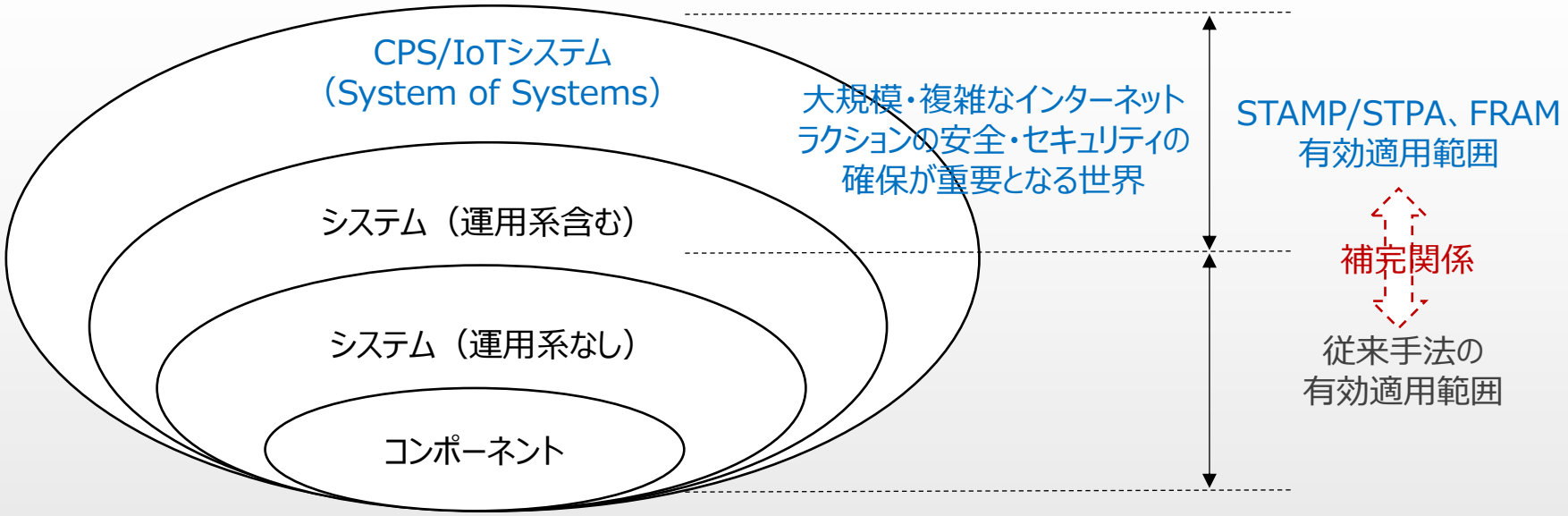
■セーフティ
偶発的なミス、故障などの悪意のない危険に対する安全を示す。

■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

■STAMP/STPA

➢目的

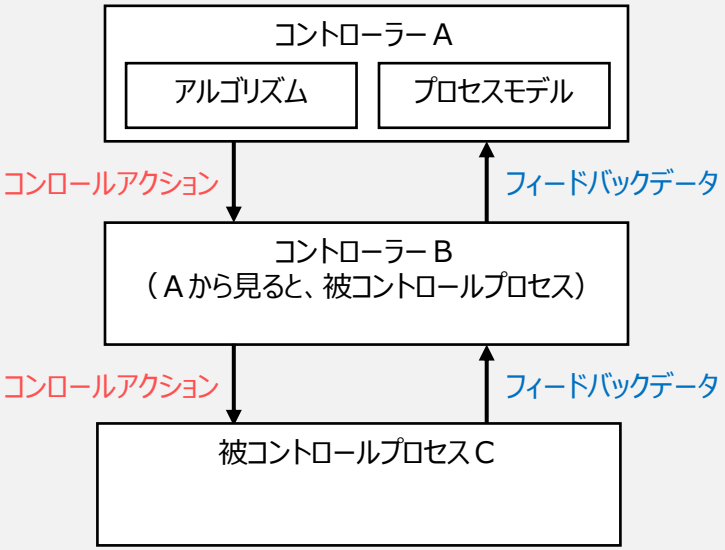
相互作用によって発生するハザードのリスクを分析する為（事前）

➢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

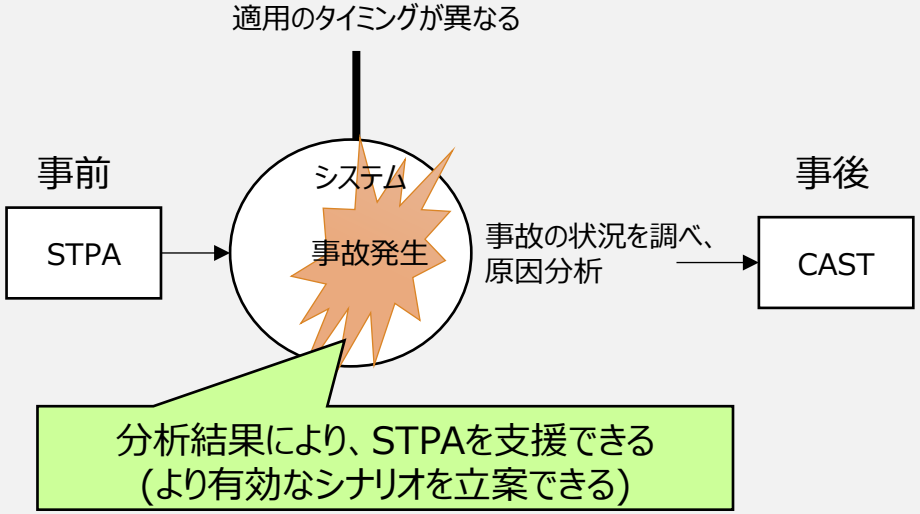
相互作用によって発生したハザードを分析する為

➢ 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(Functional Resonance Analysis Method)とは

- 目的

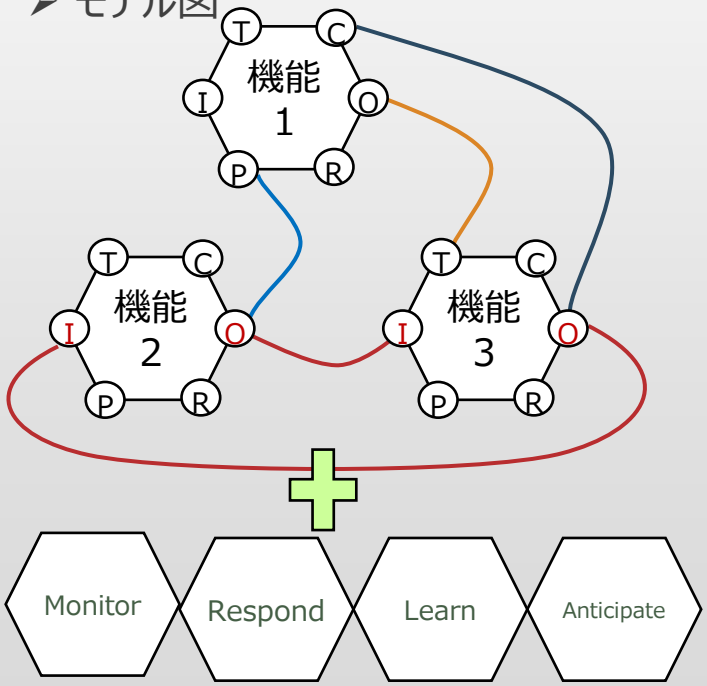
  システムの成功要因と、そこから導かれるリスク要因を発見する為

- 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

＋

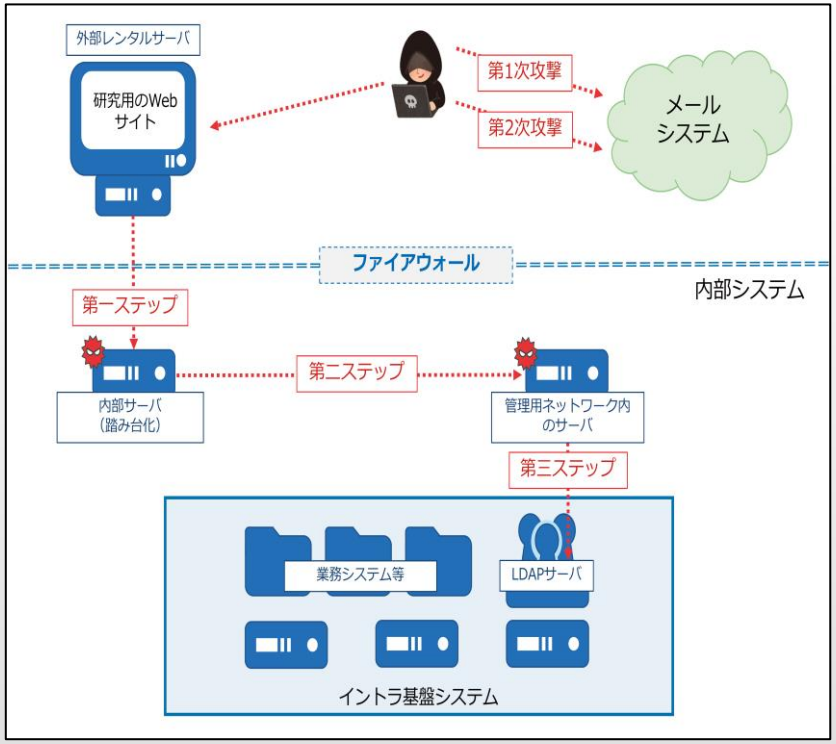
Monitor	危険な予兆を察知する能力
Respond	予兆に素早く反応できる能力
Learn	過去の成功・失敗から学ぶ能力
Anticipate	将来のリスクを予測する能力

＝

レジリエント・セキュリティの実現

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の分析結果（抜粋）

被害を発生・拡大させた要因（本文と連動）	再発防止のための対策(産総研の報告内容)		CAST分析で新たに導きだした改善案
	7.1. 現時点で措置済の対策（応急的対策）	7.2. 今後取り組む抜本的対策	
6.1.システム・機器の問題			
6.1.1 メールシステムのログイン方法	○外部からはVPN 接続を必須とする運用とし、さらに、内部ネットワークからログインする場合でも、一定期間ごとに二段階認証を求めるよう認証方式を強化した。	(同左) ※高度標的型攻撃	**●正規ユーザー認証の強化** 認証要求元が、産総研が認めた正式なユーザであることを証明できるデータを認証要求データに組み込む。 例： ワンタイムパスワードの導入 電子証明書によるアクセス元の信頼性の向上
6.1.2 内部サーバと連携していた外部サイト	○用途と通信先を精査し、必要性と安全が確認できないサーバ等は全て遮断した。	**7.2.2 運用の見直し強化** ○外部接続に際しては、ネットワーク構成、管理者の知識・能力、管理体制等について専門家による厳格な審査を行い、十分なセキュリティ対策が講じられていることを確認する。	**●アクセス内容の監視強化・監視精度向上** 外部委託業者から監視プランを提出させ、産総研の有識者が監視プラン(監視対象、異常判定条件、測定方法)に対し、妥当性確認を行った上で運用を実施するようにする **●カテゴリ毎にセキュア情報の公開範囲を限定する** 《外部委託業者》 産総研のセキュアな情報を渡さず監視業務が可能な運用を検討し作成する 例： システム・機器に直接アクセスせずとも業務可能にする仕組み 事前に開示はIDのみ、パスワードは必要時に産総研内で発行、 一定期間経過後、自動で無効化 《社内ユーザー》 ユーザに実行されて困る処理を洗い出し、その処理に必要となる情報はセキュア情報として公開しない。ユーザが実行できる処理を事実上不可能にする 上記を可能にしたのちは、前述の「●不正アクセスの検出・制御力の強化」で挙げた常時監視・常時検知・常時追従で、実行してしまった場合を摘出できるようにする
6.1.5 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	(同6.1.3)	7.2.1 システムの強化策 ○多要素認証等の強固な認証技術を、内部システムのうちイントラ基盤システム等の重要なシステムにも導入し、破られにくく、かつ攻撃が検知可能な認証システムを導入する。 ○研究用ネットワークをセグメント分離できるネットワークを構築する。さらに、セグメント間の通信を制御できるようネットワーク構成を抜本的に見直す。	●ユーザーに応じたセキュア情報の分離を強化 サーバー管理に対して、サーバー毎に管理者アカウントを設定し、他サーバーへのアクセスを制限できるようにする 例： サーバ毎に管理者のID、パスワードをユニークする サーバ毎の管理者を分離する
6.2. パスワード・暗号鍵の管理と強度の問題	○有効なパスワードの設定方法、管理方法を検討し、情報基盤部で運用開始するとともに、外部委託業者に周知・徹底した。	**7.2.2 運用の見直し強化** ○有効なパスワードの設定方法、管理方法について改めて検討し、産総研の情報セキュリティ実施要領及び情報セキュリティ実施ガイドに反映させるとともに、職員、外部委託業者に周知徹底する。	●不正アクセスの検出・制御力の強化 常時監視・常時検知・常時追従の仕組みを検討し、アクセス監視の結果を外部委託業者から産総研に常時公開し、異常値のアラート検知時に即緊急通知が出るようにする 例： 回数制限などにより自動的にIDの無効化(ロック、失効など) 電子証明書が不一致の不正アクセス パスワードミス など

弱点分析から導かれる具体的な改善

運用改善にとどまらないシステムミックな改善

STAMP/CASTの分析結果まとめ

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。

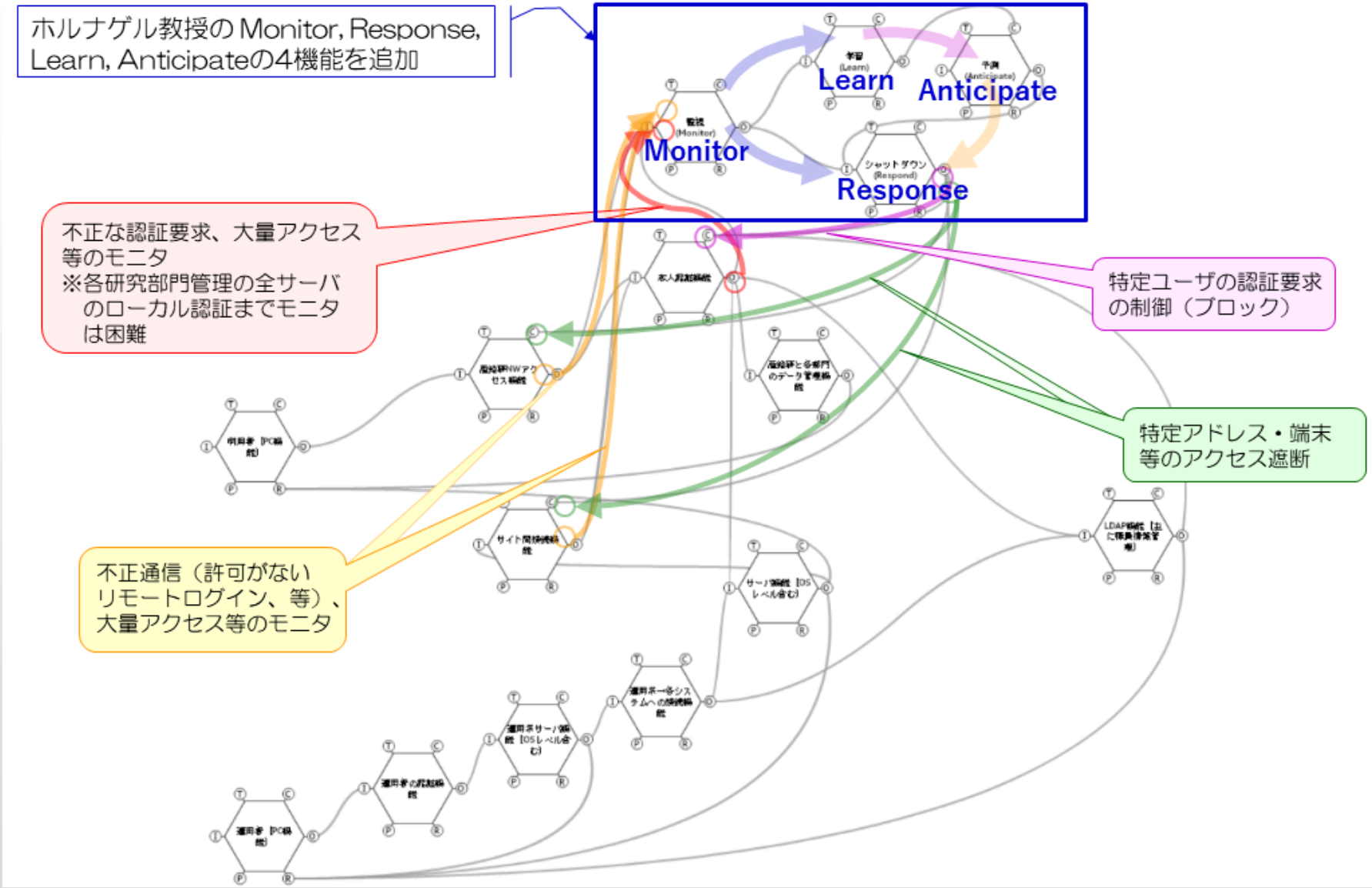
- 非安全なCAとコンテキスト要因を「同時に分析」し、問題の直接原因と発生させる背後要因を抽出できる「手順」が効果的。
- マネジメント面は、強化、見直し等の曖昧な表現になりやすいが、システミック要因分析が具体策を出すのに有効。
  例えば、マイスター認定制度導入によるスキルアップなど。

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の分析結果


ホルナゲル教授のMonitor, Response, Learn, Anticipateの4機能を追加
Learn
Anticipate
Monitor
Response
不正な認証要求、大量アクセス等のモニタ
※各研究部門管理の全サーバのローカル認証までモニタは困難
特定ユーザの認証要求の制御（ブロック）
特定アドレス・端末等のアクセス遮断
不正通信（許可がないリモートログイン、等）、大量アクセス等のモニタ

FRAMの分析結果まとめ

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。
- 静的なシステムは、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。

研究の成果まとめ

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。

本日の伝えたいことまとめ

1. セーフティの為にもセキュリティ分析が必要。

2. STAMP/CASTで網羅的に分析可能。

3. 網羅分析結果に、FRAMを加えて、セキュリティを強化。

STAMP/CAST、FRAMを現場で是非活用を！！

STAMP/STPA、FRAMの分析手順は以下の資料を参考にどうぞ

https://juse.or.jp/sqip/workshop/report/attachs/2019/iii_happyou.pdf