システムを対象とした半定量的な安全解析の試み

後藤伸寿[i]

Tentative Semi-Quantitative Safety Analysis for a System

Nobuhisa GOTO

近年開発されたシステムの多くは，ソフトウェアやネットワークが重要な役割を果たし，大規模化・複雑化が進んでいる．一方，システムは社会基盤を支え，障害(アクシデント)が発生した場合の影響が計り知れないことから，システムの安全について事前に十分な検討・解析・評価を実施することが要求される．本稿では，システム理論に基づく新しいアクシデントモデル STAMP(Systems-Theoretic Accident Model and Process)と，STAMP に基づく新しい安全解析手法 STPA(STAMP based Process Analysis)と同手法に係る動向について事例を交えて紹介し，アクシデントに発展するシナリオの発生確率を半定量化しシステムの安全解析を行うことを試みた．

(キーワード): システム，安全解析，定量化，STAMP，STPA

1 はじめに

システム [1]は，SNS といった個人間の情報交換から医療･金融等の各システムまで,社会基盤を支え，一度障害(アクシデント)が発生した場合の影響が計り知れないことから，信頼性向上の要求が高い．このため，当該システムのアクシデントがオペレーターや公衆に被害を与える恐れがないように，安全について事前に十分な検討・解析・評価を実施することが要求される．

近年開発される大規模かつ複雑なシステムにおいては，多くの場合，単一の構成要素 [2]の故障では安全が損なわれない設計となっている．一方，システムの大規模化にともない，動作も複雑化し，構成要素に故障が発生しなくても，設計者が想定していない構成要素間の相互作用が原因でアクシデントが引き起こされることがある．このようなシステムは，安全確保のための構成要素が何重にも整備されていることが多い．しかし，高い信頼性を確保するためには，2 つ以上の構成要素が同時に機能を喪失する多重故障の評価のみならず，各構成要素が想定した機能を果たしていても構成要素間の予期せぬ相互作用によって，設計者が想定したシステムの機能が果たされず最終的にアクシデントに発展する事象を評価する必要がある．

システムを対象とした安全解析手法とは，理論的に発生する可能性があると考えられるほぼ全てのアクシデントを解析する手法であり，解析結果から得られる様々な情報は一般的にリスク情報と呼ばれる．リスク情報の活用により，実際にアクシデントを発生させることなく，事前にアクシデントに発展するシナリオ及びその原因となるシステムにおける問題点を抽出し対策を施すことが可能となる．

本稿では，システムを対象とした安全解析手法の歴史背景を簡単に紹介した上で，筆者が昨今注目する，システム理論に基づく新しいアクシデントモデル STAMP(Systems-Theoretic Accident Model and Process)と，STAMP に基づく新しい安全解析手法 STPA(STAMP based Process Analysis)について簡単な事例を交えて紹介し，さらにアクシデントに至るシナリオの半定量的な解析 [3]も試みる．

2 安全解析手法の歴史背景の概要

2.1 従来手法の概要

よく知られるシステムの安全解析手法として，フ

[i] サイエンスソリューション部 社会インフラチーム チーフコンサルタント 一般社団法人日本機械学会認定計算力学技術者上級アナリスト(第 13-THFLs-0001 号)

ォールトツリー解析(FTA: Fault Tree Analysis)，イベントツリー解析(ETA: Event Tree Analysis)及びそれらを複合させた手法である確率論的リスク評価(PRA: Probabilistic Risk Assessment)，故障モード[4]影響解析(FMEA: Failure Mode and Effect Analysis), あるいは HAZOP(Hazard and Operability Studies)等がある. FTA, ETA 及び PRA については, 既報[4][5]において，各手法やさまざまな分野への適用の歴史と概要について事例を交えながら紹介した. FTA, ETA 及び PRA の特徴として，アクシデントの発生確率を定量化することが可能であり，定量化結果からシステムの安全に対する構成要素の重要度を解析する手法が確立していることが挙げられる．重要度の解析結果を参考に, システムの安全に寄与する構成要素の特定や, システムの保守・点検に係る資源の適切な配分を行うことができる.

安全解析手法におけるデファクトスタンダードと言えるこれら従来手法は, 20 世紀中頃に開発された手法である．この時代のシステムの構成要素は，機械・電気品といったハードウェアが中心であり，数が少なく，役割も明確であった．また，システムにおける人間によるオペレーションもあくまでシステムの構成要素の 1 つであり，与えられた役割も限られていた．そのため，システムのアクシデントはハードウェアの故障やオペレーションミスが根本原因であり，それが他の要素に伝搬し最終的にアクシデントに発展するものとして捉えられていた.

2.2 システムの大規模化・複雑化に伴うアクシデント発生原因の変容

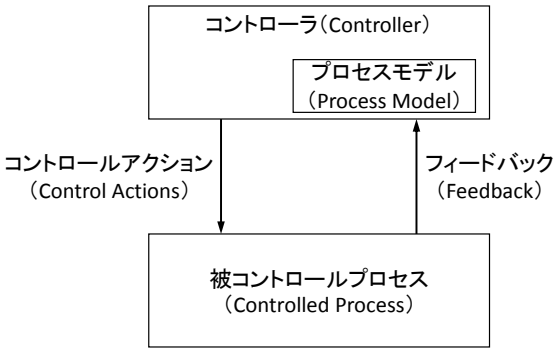
従来手法が開発された時代から数十年が経過し，近年開発されるシステムのほとんどはソフトウェアにより制御されると同時に，構成要素あるいは他のシステムがネットワークで相互に接続され連携している．このため，構成要素の数が爆発的に増大する等，大規模化・複雑化する傾向にある．また，人間の役割についても，システムにおける 1 つの構成要素としての役割を果たすにとどまらず，全体を監視し，状況に応じて適切に介入することも求められている．このため，アクシデントの発生の原因も，前述のような要素の故障やオペレーションミスに限定せず，故障あるいはオペレーションミスの発生を伴わない複数の要素間の相互作用が要因となるものについても把握することが必要となりつつある.

3 STAMP/STPA の概要

3.1 システム理論に基づく新しいアクシデントモデル STAMP

前章で述べたような背景の下, 2011 年にマサチューセッツ工科大学(MIT: Massachusetts Institute of Technology)の Leveson 教授は著書[7]の中で，システム理論に基づく新しいアクシデントモデル STAMP を提唱した.

STAMP は, システムのアクシデントは構成要素の故障のみならず，システムの中で安全のための制御を行う要素と制御される要素間の相互作用が働かないことによって起きると捉えるアクシデントモデルであり，システム理論に基づきアクシデントを説明するモデルである．図 1 に，STAMP における要素間の相互作用のモデルを示す.



※各種公開資料をもとに，みずほ情報総研が作成.

図 1 STAMP における要素間の相互作用のモデル

STAMP では，次のような前提を設けている.

- システムの安全は，安全のための制御を行う要素(Controller：コントローラ)と制御される要素(Controlled Process：被コントロールプロセス)の相互作用が適切に働くことによって実現する.
- アクシデントはコントローラから被コントロールプロセスへの必要な制御指示(Control Actions：コントロールアクション)が適切に与えられないために発生し，適切なコントロールアクションが与えられないあるいは不適切なコントロールアクションが与えられる主な要因として，コントローラ自身が想定する被コントロールプロセスの状態(Process Model：プロセスモデル)と実際の被コントロールプロセスの状態がマッチしていない.

すなわち，コントローラ及び被コントロールプロセスが故障，あるいは故障がなく仕様どおりに動作していても,それぞれの認識の不整合により，最終的にアクシデントが発生するとしている．

3.2 STAMP に基づく新しい安全解析手法 STPA

STPA は，Leveson 教授が著書 [7]の中で提案した，STAMP に基づきハザード [8]を分析する安全解析手法である．以下のような特徴があげられる．

- アクシデントを定義し，トップダウンによりアクシデントの発生原因を分析する．
- システムに係る構成要素間で相互作用が発生する複雑なシステムにおいて，アクシデントの発生原因となる適切ではない相互作用を識別する．
- 後述する 4 種類のガイドワードにより網羅的に分析する．
- システム全体のふるまいを確認しながら分析する．
- 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が可能である．

STPA の手順は大きく 3 つに分かれ，Step0 でシステム内の相互作用を明確にし，安全を実現する適切な相互作用・システムのふるまいを分析した後，Step1 でハザードを起こし得るシナリオを分析し，Step2 でシナリオが発生する要因を特定する．以下に各ステップの概要を示す.

(1) Step0

Step0 では，まず事前作業として，解析対象となるシステムについて構成要素とその役割及びシステムが正常に動作するための前提条件を整理する．

次に「準備 1」として，分析対象のシステムにおいて発生するアクシデント，ハザード，ハザードを制御するためのシステム上の安全制約 [9]を識別する．準備 1 の実施の手段として，アクシデントに対するハザードと安全制約のマトリックスを用いることが多い.

その後に「準備 2」として，安全制約の実現に関係するシステムの構成要素と構成要素間を行き来するデータやコマンドを明確化・識別し，相互作用を分析する．その結果として，コントロールストラクチャ図(Control Structure Diagram)を構築する．

図 2 にコントロールストラクチャ図のイメージを示す．このコントロールストラクチャ図は，システムの構成要素分解の粒度に応じて構築することが可能である．このため，STPA は粒度が粗い概念設計の段階からの適用が可能となる．

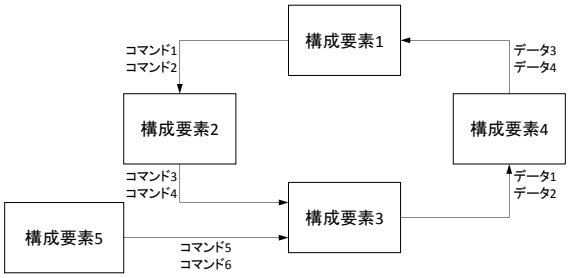


図 2　コントロールストラクチャ図のイメージ

(2) Step1

Step1 では，ハザードを起こし得るシナリオの分析を行う．具体的には，Step0 で構築したコントロールストラクチャ図から，安全制約の実行に必要なコマンドを識別し，各コマンドに対して 4 種類のガイドワード(①与えられないとハザード, ②与えられるとハザード，③早過ぎ，遅過ぎ，誤順序で実行されるとハザード，④早過ぎる停止，長過ぎる適用でハザード)を適用して, ハザードを起こし得る非安全なコントロールアクション(UCA：Unsafe Control Action)を抽出する．

UCA 抽出の手段として, 各コマンドと 4 種類のガイドワードのマトリックスを用いることが多い.

(3) Step2

Step2 では，UCA を抽出した後，UCA を発生させるシナリオを分析し, 原因を特定する. 具体的には，UCA ごとに関係するコントローラと被コントロールプロセスを識別して，シナリオ及びハザード要因(HCF：Hazard Causal Factor)を特定する．Step2 の実施の手段として，コントロールループ図を用いることが多い.

最終的には, シナリオを発生させないために, HCF に対して必要な安全要求または安全制約を定義し，対策を策定する. この HCF ごとの対策策定の作業を「Step3」と呼ぶこともある.

4 事例紹介

4.1 STPA による安全解析

身近な事象を対象とした事例として，既報 [4]で取り上げた，毎朝目覚まし時計を用いて起床している人が，朝起床することができず朝寝坊をしてしまう事象を取り上げる．

(1) Step0

アクシデント，ハザード，安全制約を識別するために，対象となるシステムの登場人物(朝起きるためのシステムの構成要素)と役割を表 1 に示す．

表 1 朝起きるためのシステムの構成要素と役割

構成要素	役割
人	・前の晩に目覚まし時計を起床時間にセットする． ・朝に自力で起床する． ・目覚まし時計が作動したならば，起床する． ・起床後に目覚まし時計の作動を解除する．
目覚まし時計	・人に起床時間がセットされる． ・起床時間になったら作動する．

対象となるシステムのアクシデント，ハザード，安全制約を識別する．アクシデントは「人が起床時間になっても起床しない」とする．各構成要素は，このアクシデントを防止するために「人は朝に自力で起床する，または前の晩に目覚まし時計をセットし，目覚まし時計が作動したならば起床する」「目覚まし時計は起床時間をセットされ，正しい時刻を指し，起床時間になったら作動する」という安全機能を持っている．ハザードはこれらの安全機能が適切に遂行されない状態であり，安全制約はそれを裏返すようにして識別することができる．ここで，ハザード「人が自力で起床しない」が考えられるが，本ハザードは，目覚まし時計の動作により起床が促されることによりハザードでなくなるため除外する．その結果，アクシデント，ハザード，安全制約を表 2 のように識別することができる．

安全制約の実現に関係するシステムの構成要素と制御の関係を明確化し，コントロールストラクチャ図を構築する．表 1 に示すとおり，構成要素は「人」と「時計」の 2 つであり，人は目覚まし時計を起床時間にセットし，目覚まし時計は起床時間に作動し人はその作動を認識し起床する関係にある．また，人は目覚まし時計のフィードバックがあった場合に起床する機能を持つ．その結果，コントロールストラクチャ図は図 3 のように構築される．

表 2 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
(A)人が起床時間になっても起床しない	(H1)人は前の晩に目覚まし時計をセットする	(SC1)人は前の晩に目覚まし時計をセットしなければならない
	(H2)人が朝起床せず目覚まし時計が作動しても起床しない	(SC2)人は目覚まし時計が作動した場合は起床しなければならない
	(H3)目覚まし時計が起床時間に作動しない	(SC3)目覚まし時計は起床時間に作動しなければならない

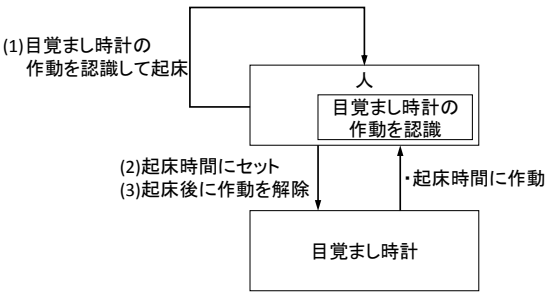


図 3 コントロールストラクチャ図の構築

(2) Step1

図 3 に示したコントロールストラクチャ図のコントロールアクションに 4 つのガイドワードを適用して UCA を抽出する．Step0 で識別した安全制約に違反するか否か識別した結果，表 3 のように 4 つの UCA が抽出された．ここで，独立行政法人 情報処理推進機構が発行している解説書(以下，「IPA 解説書」という)[10]に倣って，UCA にはコントロールアクションの番号と適用したガイドワードが分かるように以下のような識別子を付与した．

UCAn-N/P/T/D

ここで，n：コントロールアクションの番号，
N：与えられないとハザード，
P：与えられるとハザード，
T：早過ぎ，遅すぎ，誤順序で実行されるとハザード
D：早過ぎる停止，長すぎる適用でハザード．

表 3　UCA の抽出

No.	コントロールアクション	与えられないとハザード(N)	与えられるとハザード(P)	早過ぎ，遅すぎ，誤順序で実行されるとハザード(T)	早過ぎる停止，長すぎる適用でハザード(D)
1	起床時間にセット	(UCA1-N)目覚まし時計が起床時間に作動しない(SC1 違反)	ハザードにならない	ハザードにならない (目覚まし時計のセットの実行の時期や誤順序は非常に稀有と仮定)	適用対象外 (本コマンドは継続して適用されない)
2	目覚まし時計の作動を認識して起床	(UCA2-N)目覚まし時計の作動を認識しない，あるいは認識しても起床しない(SC2 違反)	ハザードにならない	(UCA2-T)目覚まし時計の作動を認識しても，起床時間より遅く起床する(SC2 違反)	適用対象外 (本コマンドは継続して適用されない)
3	起床後に作動を解除	ハザードにならない (起床後に目覚まし時計の作動が継続するのみ)	ハザードにならない	(UCA3-T)二度寝等，起床と作動の解除の順序を間違えるとハザード(SC3 違反)	適用対象外 (本コマンドは継続して適用されない)

(3)　Step2

シナリオ及びHCFを特定するにあたり，まずUCAごとにコントロールループ図を作成して，シナリオをコントローラ及び被コントロールプロセスに記入した．ここで IPA 解説書 [10]に倣って，STPA の手順で示されている以下のガイドワードを適用し，シナリオを特定した．

① コントローラに関するもの：
　不十分な制御アルゴリズム
② コントロールアクションに関するもの：
　コントロールアクションが不適切・無効・欠落
③ プロセスモデルに関するもの：
　プロセスモデルが不一致，不完全
④ 被コントロールプロセスに関するもの：
　部品故障，経時変化
⑤ フィードバックに関するもの：
　フィードバックの不十分・欠落・遅延

また，特定した各シナリオに以下のような識別子を付与した．

HSn-N/P/T/D-m

ここで，n：コントロールアクションの番号，
　　N：与えられないとハザード，
　　P：与えられるとハザード，
　　T：早過ぎ，遅すぎ，誤順序で実行されるとハザード
　　D：早過ぎる停止，長すぎる適用でハザード，
　　m：UCA ごとに導出したハザードシナリオの連番．

(a)　UCA1-N に至るシナリオ

コントロールアクション 1 番に関する UCA に至るシナリオ特定のためのコントロールループ図を図 4 に示す．コントロールアクション 1 番に関する UCA に至るシナリオとして，4 つのシナリオを特定することができた．

(b)　UCA2-N，UCA2-T に至るシナリオ

コントロールアクション 2 番に関する UCA に至るシナリオ特定のためのコントロールループ図を図 5 に示す．コントロールアクション 2 番に関する UCA に至るシナリオとして，4 つのシナリオを特定することができた．

(c)　UCA3-T に至るシナリオ

コントロールアクション 3 番に関する UCA に至るシナリオ特定のためのコントロールループ図を図 6 に示す．コントロールアクション 3 番に関する UCA に至るシナリオとして，1 つのシナリオを特定することができた．

(UCA1-N)目覚まし時計が起床時間に作動しない(SC1 違反)

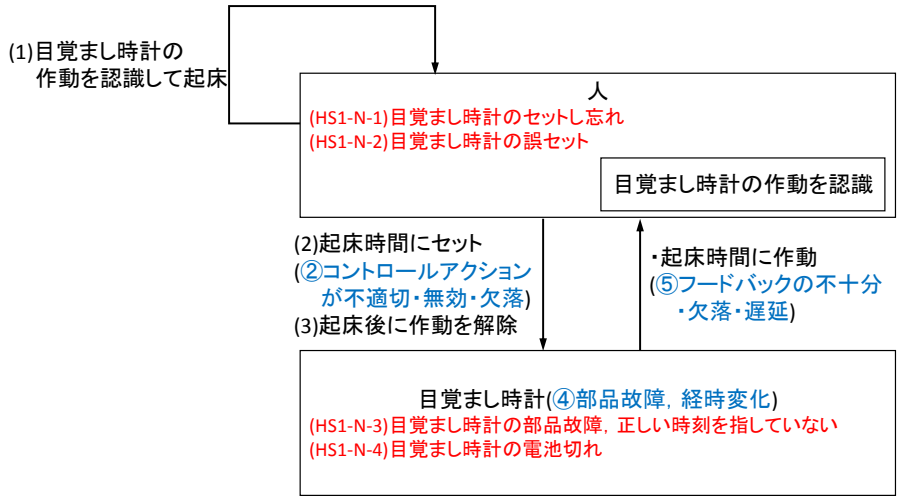


図 4　UCA1-N のコントロールループ図

(UCA2-N)目覚まし時計の作動を認識しない，あるいは認識しても起床しない(SC2 違反)
(UCA2-T)目覚まし時計の作動を認識しても，起床時間より遅く起床する(SC2 違反)

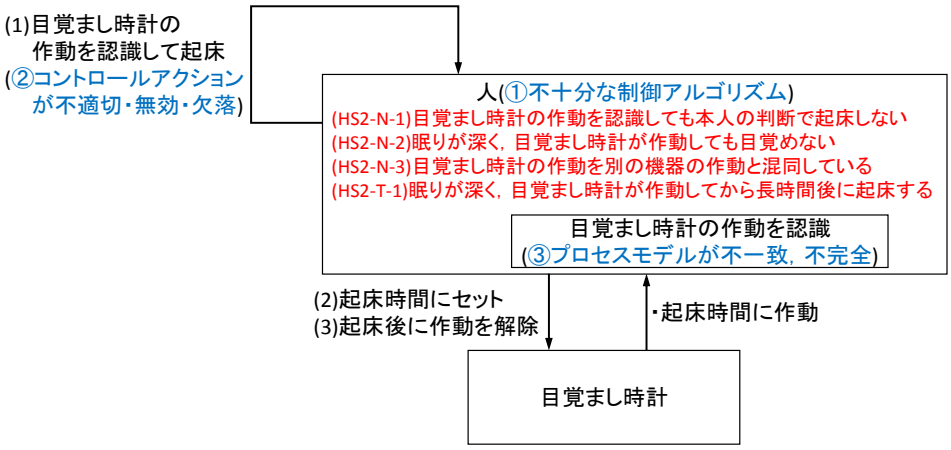


図 5　UCA2-N，UCA2-T のコントロールループ図

(UCA3-T)二度寝等，完全に起床しない状態で作動を停止するとハザード(SC3 違反)

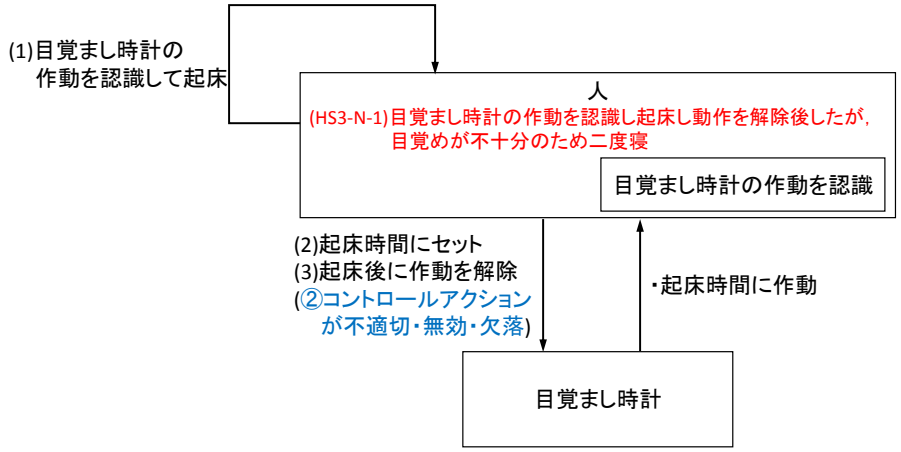


図 6　UCA3-T のコントロールループ図

上記(a)～(c)のシナリオ及びシナリオに対応したHCFを整理した一覧表を表 4 に示す. 今回の解析では，人自身の問題の HCF が最も多かった．特に，人自身の HCF によるシナリオは，同様の事象を PRA で解析した既報 [4]において特定していなかったシナリオを 5 つ新たに特定することができた．これは，PRA あるいは FT や ET では，アクシデントの原因を機器の故障や動作不良やヒューマンエラーと捉えるため，システムのモデル化において人自身の問題の考慮が抜けていたこと，STPA では，コントロールストラクチャ図を作成することにより,「人による目覚まし時計の解除」というコントロールアクションや「コントローラの不十分な制御アルゴリズム」というガイドワードを適用することにより，人自身の問題を新たに考慮することができたことが要因と考えられる．

表 4　シナリオ及び HCF の一覧

HCF	シナリオ
目覚まし時計の問題	(HS1-N-3)目覚まし時計の部品故障，正しい時刻を指していない
	(HS1-N-4)目覚まし時計の電池切れ
人の指示間違い	(HS1-N-1)目覚まし時計のセットし忘れ
	(HS1-N-2)目覚まし時計の誤セット
人自身の問題	(HS2-N-1)目覚まし時計の作動を認識しても本人の判断で起床しない
	(HS2-N-2)眠りが深く，目覚まし時計が作動しても目覚めない
	(HS2-N-3)目覚まし時計の作動を別の機器の作動と混同している
	(HS2-T-1)眠りが深く，目覚まし時計が作動してから長時間後に起床する
	(HS3-N-1)目覚まし時計の作動を認識し起床し動作を解除したが，目覚めが不十分のため二度寝

※赤字は，同様の事象を対象とした PRA による解析 [4]で特定していなかったシナリオ.

4.2　シナリオの半定量化の試行

前述のとおり，PRA ではアクシデントの発生確率を定量化することが可能であり，表 4 に黒字で示した 4 つのシナリオは既報 [4]において表 5 のように定量化を行っている．

表 5　目覚まし時計の問題，人の指示間違いの発生確率

シナリオ	確率	確率の算出根拠
(HS1-N-3)目覚まし時計の故障	2.74×10^{-4}	10 年間使用していて，1 度だけ故障
(HS1-N-4)電池切れ	5.48×10^{-4}	標準的な電池で 5 年間作動
(HS1-N-1)目覚まし時計をセットし忘れ	1.10×10^{-2}	ここ半年で 2 度あった
(HS1-N-2)目覚まし時計の誤セット	5.48×10^{-3}	ここ半年で 1 度あった

今回，STPA により新たに特定した 5 つのシナリオに対し半定量化を試みる．これら 5 つのシナリオの発生確率を厳密に特定(定量化)することは困難と考えられるが，表 6 のように各シナリオの起こりやすさを相対的に設定する(半定量化)．さらに，これら 5 つのシナリオは「目覚まし時計が作動したにもかかわらず，本人の問題で起床しなかった」ものであり，目覚まし時計が作動した場合に起きる/起きない相対的な起こりやすさを 9 対 1 と設定する．これにより，目覚まし時計が作動した場合の全シナリオの相対的な起こりやすさを設定することができる．

ここで既報 [4]では，目覚まし時計が正常作動する頻度を 172 回/年と定量化している．この頻度に対し設定した相対的な起こりやすさを適用することにより，各シナリオの頻度を算出することができる(表 6).

さらに, 各シナリオの重要度を評価するために FV 重要度を算出した．FV 重要度は，以下の式から算出され，当該系統または機器が事故の発生頻度に関与している割合を示す指標で，当該系統または機器の信頼性向上効果の把握に有効な指標である．

$$FV_a = \frac{F - F_{a=0}}{F}$$

ここで，FV_a :事象 a に対する FV 重要度,
F ：事故の発生頻度,
$F_{a=0}$ ：事象 a の発生確率を 0 とした場合の事故の発生頻度.

FV 重要度の算出結果を図 7 に示す．元々の発生確率が大きい「二度寝」「目覚ましが作動してから長時間後に起床」あるいは「目覚まし時計セットし忘れ」となっている．

表 6　人自身の問題が原因の 5 つのシナリオの相対的な起こりやすさの設定

シナリオ	相対的な 起こりやすさ①	相対的な 起こりやすさ②	頻度 (回/年)
(HS2-N-1)目覚まし時計の作動を認識しても本人の判断で起床しない	0.5	0.05	0.86
(HS2-N-2)眠りが深く，目覚まし時計が作動しても目覚めない	1	0.1	1.7
(HS2-N-3)目覚まし時計の作動を別の機器の作動と混同している	0.5	0.05	0.86
(HS2-T-1)眠りが深く, 目覚まし時計が作動してから長時間後に起床する	3	0.3	5.2
(HS3-N-1)目覚まし時計の作動を認識し起床し動作を解除したが，目覚めが不十分のため二度寝	5	0.5	8.6
目覚まし時計の作動により起床	－	9	155
		合計	172

※・相対的な起こりやすさ①：5 つのシナリオの発生の蓋然性の相対値.
・相対的な起こりやすさ②：目覚まし時計の作動により起床するシナリオも含めた，6 つのシナリオの発生の蓋然性の相対値.

図 7　FV 重要度の算出結果

こういった重要度を算定することにより，アクシデントに至るシナリオを特定するにとどまらず，アクシデントの発生に寄与するシナリオを評価し，評価結果に基づき対策の優先順位等を策定することが可能となる.

なお，STPA により特定したシナリオを定量的に評価する研究が進められており，2016 年 12 月に九州大学にて開催された第 1 回 STAMP ワークショップ in Japan にて（株）京三製作所が鉄道システムを対象とした手法について発表[11]を行っている．同手法では，HCF を特定した後に Step3 を実行し，シナリオが発生しないための制約事項を設定，設定した制約事項をもとに対策の検討を行い，対策の効果を FMEA で解析している.

5　おわりに

システム理論に基づく新しいアクシデントモデル STAMP と STAMP に基づく新しい安全解析手法 STPA について，安全解析手法の歴史背景や簡単な

事例も交えて紹介し，半定量的な解析の試行を行った．

STPA は近年開発された大規模かつ複雑なシステムに潜在するハザードを抽出し分析することを可能とするツールとして，開発された米国を中心に，主に航空宇宙，自動車，医療，エネルギー等の制御システムを対象として実績を積み上げており，今後様々な分野における普及が見込まれる．特に自動車分野では ISO26262 の 2nd Edition で STPA の記載が予定されていることから，日本においても普及の拡大が予想される．一方，エンタープライズ系等，適用研究の段階の分野もあるほか，抽出したシナリオの定量化結果に基づいたシステムの安全に対する重要度の高い構成要素の特定等，今後の手法の改良・発展が期待される．

近年，システムの大規模化・複雑化に伴う社会への影響の拡大や気候変動等による災害の増加に伴い安全解析の重要性が増しており, STPA のみならず，安全解析手法全般において幅広い分野への更なる展開が期待される. みずほ情報総研 サイエンスソリューション部においても，これまでの業務経験に基づいて蓄積してきた技術等を活かして，安全解析関連業務を通じて社会に貢献していきたいと考えている．

引 用 文 献

1) ここでは，「特定の目的を成し遂げるための，相互に作用する複数の要素を組み合わせたもの」を意味する．
2) ここでは，「機器・設備・ソフトウェア・人間等のシステムの設計・開発・運用に係る全て」を意味する．
3) ここでは，「おおよその値を測定する」ことを意味する．
4) 後藤，重盛 : 確率論的安全評価手法について，みずほ情報総研技報，4，No.1(2012).
5) 後藤，重盛 : フォールトツリー解析及びイベントツリー解析によるリスク評価の」事例，みずほ情報総研技報，7，No.1(2015).
6) ここでは，「断線，短絡，折損，摩耗，特性の劣化といった故障状態の形式による分類」を意味する．
7) Leveson, Nancy G. : Engineering a Safer World - Systems Thinking Applied to Safety, Cambridge, Massachusetts: The MIT Press (2011).
8) ここでは，「アクシデントが潜在している状態」を意味する．
9) ここでは，「アクシデントを回避するためにハザードを制御するシステム上の制約」を意味する．
10) 独立行政法人情報処理推進機構 : はじめての STAMP/STPA(実践編)～システム思考に基づく新しい安全性解析手法～Ver.1.0(2017.3).
11) 高田 : STAMP 解析での定量的評価と STAMP 解析の開発プロセスにおける適用段階，第 1 回 STAMP ワークショップ in Japan (2016).