論　　文

Dual Vee Model を用いた大規模複雑システム事故の根本原因解析

前島弘則†・神武直彦†
狼嘉彰†・高野研一†

システムで発生した不具合，事故の根本原因解析は，当該システムにおける再発防止対策及び類似システムへの水平展開の観点で重要である．解析手法としては，なぜなぜ分析や故障の木分析等が広く用いられているが，ブレインストーミング的な手法であるため，解析結果は解析者のスキルに大きく依存する．筆者らは，解析を進める際のガイダンスを与えることにより解析者のスキルへの依存度を軽減する手法として，宇宙機システムに適用することを目的として，Dual Vee Model を用いた根本原因解析を提案してきたが，本論文では，当該手法を原子力発電所の事故に適用した結果を示す．また，当該手法が適用可能な対象システムを識別するための分類チャートを考察する．

キーワード：根本原因解析，Dual Vee Model，原子力発電所，システム，事故

1. はじめに

システムが大規模かつ複雑になるにつれて，ひとたび不具合が発生すると，大きな事故に発展する事例が多く見られるようになっている．原子力発電所，化学プラント，鉄道，宇宙機などの事例がそれに対応する．大規模かつ複雑なシステムでは，多くの構成要素が複雑に関連しているため，ある要素で発生した不具合が別の要素の不具合に連鎖する場合があり，発生した不具合の原因究明は容易ではない．

一般に，不具合・事故の原因は次の二種類に分類される[1]．

1）直接原因：不具合・事故の直前の事象・状況（複数の場合もある）であり，それを改善することでシステムを正常状態に復帰することができるもの．原因解析は，リアルタイムで行われる．

2）根本原因：直接原因の背景となる，組織・プロセスに起因する要因．原因解析は，オフラインで行われる．

直接原因は，当該システムを正常復帰させるためにタイムリーに解析する必要がある．他方，根本原因は，直接原因事象の背後要因であり，適切な是正を行わない限り，類似システムにおいて同様な事故が繰り返し発生する可能性がある．したがって，根本原因解析はきわめて重要である．根本原因解析の手法としては，原因影響解析図，マトリクス法，なぜなぜ分析，故障の木解析（FTA）等が一般的である[2]．その中で，様々な業界においてもっとも広く用いられているのが，なぜなぜ分析[3]及び故障の木解析[4]である．しかし，これらの手法は，分析者の経験と知識に依存するブレインストーミングから出発するものであり，分析者は対象となるシステムを熟知している必要がある[5]．また，これらの手法には，分析を進めるためのガイダンスがないため，原因候補を網羅的に抽出することが困難であることが指摘されている[6]．

著者らは，上述の欠点を克服するものとして，Dual Vee Model を根本原因解析に適用することを提案し，宇宙機システムの軌道上不具合の根本原因究明に有用であることを，実例を用いて実証している[7]．Dual Vee Model は，Forsberg と Mooz が提唱した，ライフサイクルを表現するモデルであり，システムズエンジニアリング手法を用いて開発が行われる大規模システムによく適合する[8]．

本論文では，宇宙機システムのために考案された Dual Vee Model を用いた根本原因解析手法を，過去の原子力発電所事故の実例に適用して根本原因を抽出し，再発防止策の案を検討する．これにより，提案手法が，宇宙機より大規模なシステムである原子力発電所にも有効に用いることができること，すなわち，従来手法の欠点である，分析者が対象となるシステムを熟知している必要があること，分析を進めるためのガイダンスがないため原因候補を網羅的に抽出すること

2012 年 9 月 18 日　原稿受付，2013 年 1 月 21 日　受理
† 慶應義塾大学大学院 システムデザイン・マネジメント研究科　〒 223-2458　横浜市港北区日吉 4-1-1
E-mail：hmaejima@z8.keio.jp

が困難であること，を改善できることを示す．さらに，当該手法が適用可能な対象システムの範囲を明確にするため，各種システムが有する性質をもとにした分類チャートを考察する．

2.　根本原因解析の適用事例

2.1　宇宙機システム

宇宙機システムは最も複雑なシステムのひとつである．その開発はシステムズエンジニアリングの手法を用いて基準化され，信頼性の向上が図られている[10]．しかし，高信頼性を目指した設計製作試験を実施しているにも関わらず，無重力，真空，高低温等の軌道上の特殊な環境を完全に模擬して試験をすることが困難であることもあり，多くの軌道上の不具合・事故が報告されている[11), 12)]．

軌道上不具合・事故の根本原因解析の手法としては，なぜなぜ分析や FTA を用いることが標準となっている[1), 13)]．しかし，なぜなぜ分析や FTA は，分析者の経験と知識に依存する手法であり，分析を進める上で必要なガイダンスがないため，原因候補を網羅的に抽出することが困難である．対策のひとつとして，FTA にガイダンスとして時間軸の要素を取り込み，開発フェーズのプロセスを表現する研究が発表されている[14)]．FTA におけるこの欠点は，安全解析の分野でも指摘され，対象システムをコントロールとモニタで表現することにより解析のためのガイダンスとする手法である STAMP/STPA が提唱され，有人宇宙機における有効性を確認している[15)]．

筆者らは，従来，宇宙機システムの根本原因解析に用いられてきた手法の欠点を改善するため，Dual Vee Model を用いた根本原因解析を提案した[7)]．Dual Vee Model は，システムのライフサイクルを表現する手法であり，Architecture Vee 及び Entity Vee と呼ばれる「V」字型の枝を立体的に組み合わせたものである．Architecture Vee は，システム，サブシステム，コンポーネント等のプロダクトの構成レベルを表現する．「V」の左側で，下位レベルへの要求のフローダウン（分解）を表す．「V」の右側では，下位レベルから上位レベルへのインテグレーション（統合），すなわち，コンポーネントをサブシステムに統合し，サブシステムをシステムに統合する様を示す．Entity Vee は，各レベルのプロダクトの要求・設計・製作，組立・試験・検証のプロセスを表現する（**Fig.1**）[16)]．

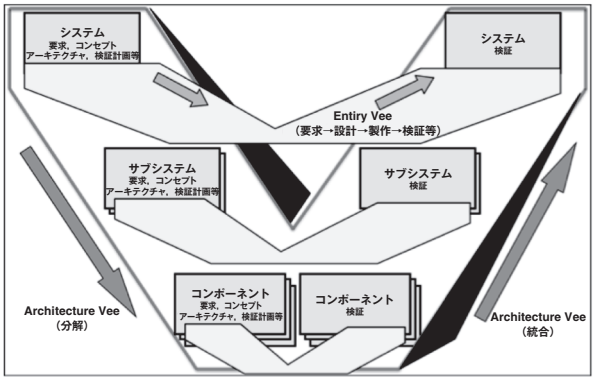

Fig.1　Dual Vee Model [16)] を和訳修正

宇宙機システムの開発は，システムズエンジニアリングを導入し，Architecture Vee と Entity Vee のフローを厳密に適用して行われるため，Dual Vee Model により極めて良好に表現できる．通常，Dual Vee Model は，システム開発段階において開発プロセスのフローを定義することを目的として，「V」の左上から右上に向かって，開発プロセスを時系列に並べることで，プロセス相互の関係を可視化するために使用する．しかし，根本原因解析に Dual Vee Model を適用する場合は，運用フェーズから時間を遡って，「V」の右上から左上に向かって辿る．Dual Vee Model を用いることにより，宇宙機システムの開発プロセス全体を可視化することができるため，すべてのプロセスを時系列順にひとつずつ検討することができ，全プロセスを漏れなく検討するためのガイダンスとなる．これにより，不具合・事故の根本原因となったプロセスがどれにあたるのかを効率的に抽出することができる．

筆者らは，実際に地球観測衛星「みどり 2」の 2 件の軌道上不具合の根本原因解析を，Dual Vee Model を用いて実施し，提案手法の有効性を示した[7)]．提案手法と従来手法の解析結果比較サマリを **Table 1** に

Table 1　Comparison between the proposed method and the conventional method [6)]

不具合事例	提案手法	従来手法
回転構造体からの反射波によるマルチパス不具合	・システムコンセプトが不十分だったため，回転構造体のシステムレベル検証（試験または解析）の要求が不十分となった ・設計審査において不具合の可能性を識別できなかった組織的問題があった	・展開及び回転体のマルチパスに関する知識の不足
不適切な熱設計と非接地 MLI に起因する電力喪失不具合	・コンポーネントレベルの知識の不足，不十分な検証要求，設計審査の不足	・コンポーネントレベルにおいて十分な検査及び設計審査が行われなかった（設計者及び審査員が電力ハーネスの熱設計と放電に十分な注意を払わなかった）

示す．「回転構造体からの反射波によるマルチパス不具合」については，従来手法が知識不足を指摘するに留まっていたのに対し，提案手法はシステムコンセプトが不十分であったこと及び設計審査の問題を抽出することができている．「不適切な熱設計と非接地 MLI に起因する電力喪失不具合」については，従来手法と提案手法とも，知識不足，検証不足，審査不足を抽出している．このように提案手法は，従来手法による根本原因候補に比べて同等，または従来手法では識別できなかった根本原因候補を挙げることができており，より網羅的な解析が可能であることを示している．

2.2 原子力発電所

原子力発電所は，事故の根本原因解析手法が最もよく研究されている大規模システムのひとつであり 9)，また，解析の結果が多く公開されている．米国エネルギー省（DOE）は，根本原因解析のためのガイドラインを出版しており，最も共通的に用いられる手法として，Events and Causal Factor Analysis, Change Analysis, Barrier Analysis, Management Oversight and Risk Tree（MORT）Analysis, Human Performance Evaluation, Kepner–Tregoe Problem Solving and Decision Making を挙げている（**Table 2**）[17]．

また，国際原子力機関（IAEA）は，原子力発電所の事故に用いる主要な根本原因解析ツールとして，HPES（Human Performance Enhancement System），MORT（Management Oversight and Risk Tree），SOL（Sicherheit durch Organisationales Lernen），ASSET（Assessment of Safety Significant Event Team），MTO（Man, Technology, Organization）を挙げている [18]．いずれも，他のシステムの原因解析で一般的に用いられている FTA と異なり，運用，管理，組織の解析に重点を置いている点が特徴である．Embrey[19] や Ghosh ら [20] も，システムの安全性の確率論的解析にマネジメント及び組織の要因を取り入れることを提案している．

国内においても，原子力安全・保安院は，「これまでの事業者の不具合是正の取組が表面的，すなわち，顕在化した事象の改善にとどまり，組織要因を中心とする根本的な原因を分析，改善する活動が十分には行われていなかったために，根本的な原因を残したままに組織要因を原因の一つとする事故，トラブルが絶えない」と指摘し，根本原因解析において組織要因に着目することを重要視している [21]．さらに，佐藤らは，IAEA が提唱する前述の ASSET 及び MORT について，「こうした分析にはある程度の経験と知識が必要であり，専門化の領域に入ってくる．根本原因分析では，分析者個人の技量に依存する傾向にあるが，その技量による分析結果への影響を最小限に抑えることができるような手法を整備することが必要である」とし，認知行動過誤原因分析手法，4M5E マトリックス型分析手法を提唱している [22]．

一方で，原子力発電所は海外の技術を用いたものも多いため，発生した事故の原因解析をシステムの設計にさかのぼって実施できず，運用に起因するものとして終わらせるケースも見受けられる．

3. Dual Vee Model を用いた根本原因解析手法

3.1 提案手法の原子力発電所の事故への適用

2.1 に示したとおり，筆者らが提案した Dual Vee Model を用いた根本原因解析手法は，宇宙機の軌道上事故によく適用できることを報告している．ここでは，原子力発電所の事故へ適用した結果を示す．

3.1.1 浜岡原子力発電所 1 号機の配管破断事例

平成 13 年 11 月 7 日，浜岡原子力発電所 1 号機において，高圧注入系手動起動試験を実施したところ，衝

Table 2 Summary of RCA Tools [17]

手法	用途	利点	欠点	備考
Event and Causal Factor Analysis	長く複雑な原因要素チェーンを有する多面的な問題	解析プロセスの視覚化，条件への寄与の識別	プロセスに精通している者が必要，長時間を要する	事象の広範な知見が必要
Change Analysis	原因が不明瞭なとき，特に機器の不具合に有効	単純な 6 ステップのプロセス	自明の解となる恐れ	すべての原因が識別されない可能性
Barrier Analysis	バリア，機器の不具合，手順や組織の問題	システム的なアプローチ	プロセスに精通している者が必要	MORT Hazard ／ Target コンセプトの基礎
MORT	再発不具合で専門家が不在の場合，プログラマチックな問題	質問リストが用意されるため事前のトレーニングがなくても使える	特定原因ではなく原因のエリアの識別に留まる可能性	問題のエリアの特定に失敗したときは cause and effect analysis[2] を使う
Human Performance Evaluations	人が関わる場合	徹底的な解析	プロセスに従えば特になし	トレーニングが必要
Kepner–Tregoe		構造的アプローチ	必要以上に複雑になる可能性	トレーニングが必要

Note）RCA：Root Cause Analysis

撃音が発生すると共に，高圧流入系ポンプがトリップした．事業者は，翌日，原子炉を高圧停止した．その原因は，原子炉水の放射線分解により発生した水素と酸素を含む主蒸気が余熱除去系蒸気凝縮系配管の閉塞部に蓄積，高温の蒸気層と低温の非凝縮性ガス層との分離が生じたところに，高圧注入系の起動試験時に当該配管内に生じた圧力変動によって高温の蒸気が非凝縮性ガス側に流入し，配管内面に付着していた貴金属の触媒作用の助けもあって着火に至り，配管が破断したものと推定された．平成 5-6 年に，余熱除去系蒸気凝縮系配管を別の不具合のために改造したことにより，非凝縮性ガスが滞留しやすい構造となったことがこの事故の背景にある．この配管の改造を実施した際，非凝縮性ガスの問題については，開発者である米国企業によってベント系及び再結合器による対策がとられていることから，技術的に対応済みと考えられており，非凝縮性ガスの滞留を問題視しなかったとされている．再発防止対策としては，設計の原点に立ち戻った技術的検討を行うこと，事故・トラブルの発生の背景や技術の品質保証，品質管理活動にまで目を向けた検討を行うこと，現在の「設計管理指針」を見直すこと，技術管理やリスク管理を専門に行う組織の設置とこの職務を主たる責任とする経営陣の選任等の組織的な取り組みを行うこと，が提言された [23]．

以下，公開されている情報のみをもとに，Dual Vee Model を用いた根本原因解析を行った結果を示す．**Fig.2** のように，原子炉をシステム，余熱除去系蒸気凝縮系をサブシステム，配管をコンポーネントと位置付ける．それぞれのレベルにおいて，Entity Vee として，要求プロセスから検証プロセスに至るフローを順に記述している．各レベルの設計プロセスを上下に貫く上向き矢印は，基本設計審査の流れを表す．基本設計審査は，上位レベルからの要求フローダウンを審査するため，システムレベルの審査を先に，下位レベルの審査を後に実施する．Fig.2 は，時間を遡って根本原因を検討する様を示しているため，矢印の向きが審査実施の順とは逆になっている．詳細設計審査は，製作及びインテグレーションを審査するため，下位レベルの審査を先に，システムレベルの審査を最後に実施する．

配管の破断事象が，どの開発プロセスに問題があったために発生したのか，本来はどのプロセスで発見されるべきであったのか，を順に検討する．まず，システムレベル（原子炉）の検証（試験・解析等）は，全体の運用模擬試験等であり，長時間運用後に発現する事象を発見することは困難である．従って，システムレベルの開発プロセスに問題はなかったものと考えられる．同様に，システムにインテグレーションされる前のサブシステムレベル（余熱除去系／蒸気凝縮系）の検証で発見することも困難であるため，サブシステムレベルの開発プロセスにも問題はなかったものと考えられる．最後に，コンポーネントレベルである配管

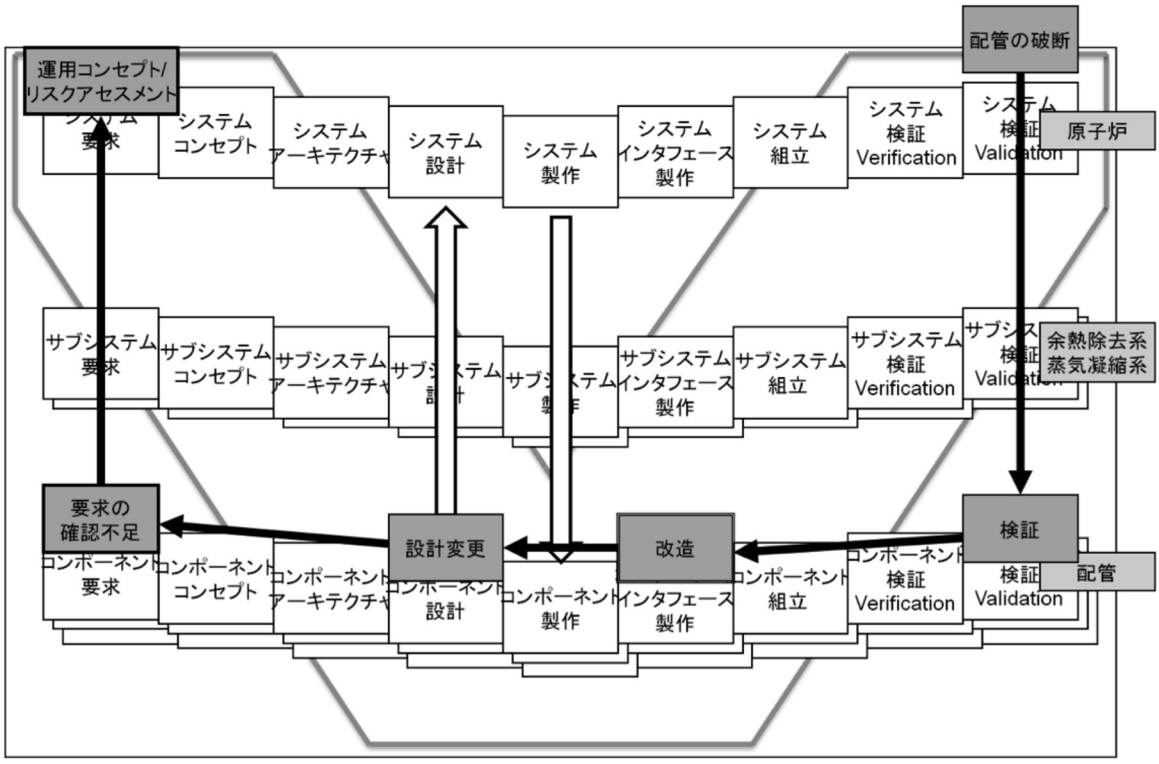

Fig.2　A root cause analysis result of a NPP pipe failure using Dual Vee Model

の開発プロセスを検討する．この事故は，改造した配管の設計に起因することがわかっている．改造にあたり，これまでの設計を見直す際には，コンポーネントへの要求に遡って検討することが重要である．さらに，コンポーネントへの要求は上位レベルからフローダウンして制定されているものであるため，システムレベルの運用コンセプトを再確認することにより，改造が他の機能性能に影響を与えるかどうか検討することが重要である．非凝縮性ガスの問題は，開発者である米国企業により技術的に対応済みと考え問題視しなかったとされていたとの報告があるため，リスクとして識別されていなかったものと考えられる．もし，非凝縮性ガスの問題をシステム要求プロセスにおいてリスクとして識別していれば，設計変更時に要求を再確認する際に，考慮すべき事項として気付くことができた可能性がある．このように，Dual Vee Model を用いることにより，対象システムを，システム，サブシステム，コンポーネントに分け，すべての開発プロセスを網羅的に検討し，システム要求プロセス及びコンポーネント要求プロセスに改善が必要である可能性を抽出することができた．再発防止対策としては，非凝縮性ガスの滞留のリスク識別不足が原因であった可能性に鑑み，システム要求プロセスのリスク識別を十分に行うこと，また設計変更にあたってはそのコンポーネントの設計要求を確認するのみならず，より上位レベルの運用要求，リスクを再確認することを提言することができる．

3.1.2　浜岡原子力発電所 5 号機の動翼亀裂事例

平成 18 年 6 月 15 日，浜岡原子力発電所 5 号機はタービンの軸振動の過大により原子炉が自動停止した．原子力安全委員会資料[24]によれば，原因究明の結果，試運転中の 20％負荷遮断試験時にランダム振動及びフラッシュバック振動が重畳したことにより，動翼フォーク部に亀裂が発生し，その後の無負荷及び低負荷運転中のランダム振動応力と，各負荷遮断試験等によるフラッシュバック振動応力により，亀裂が進展したものと推定された．根本原因としては，開発当時，低負荷時に第 12 段動翼までランダム振動が及ぶことが認識されず，またフラッシュバック振動と重畳するという事象が想定できなかったとされている．それを踏まえて，再発防止対策として，従来知見の適用の妥当性について十分精査した上でモデル試験の適用範囲を決定すること，モデル試験計画時に実機を模擬していない項目をリストアップし，開発デザインレビュー等で十分評価すること，これらをメーカのタービン設計部門の基準に反映させること，等を行うこととされた．

以下，公表されている情報をもとに，Dual Vee Model を用いて根本原因解析を実施した結果を示す．**Fig.3** に示すように，原子炉をシステムとしてとらえたとき，タービンはサブシステム，動翼はコンポーネ

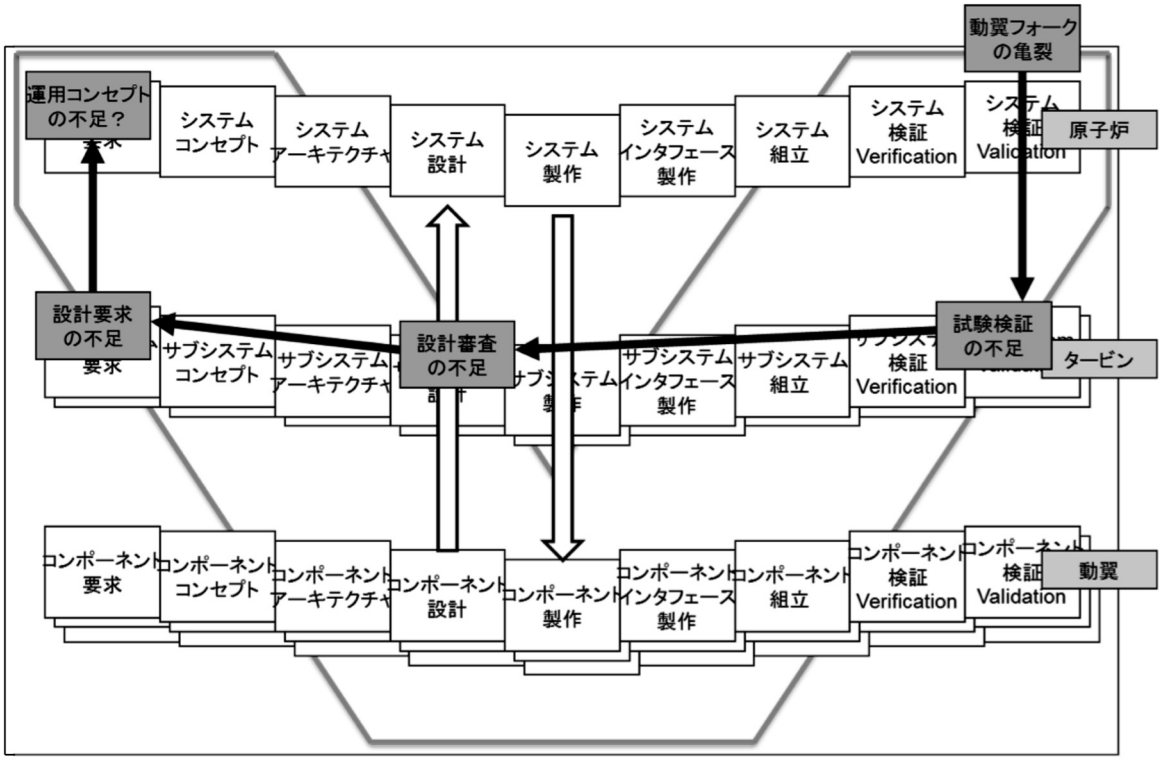

Fig.3　A root cause analysis result of a NPP rotor blade failure using Dual Vee Model

ントと位置づけられる．動翼フォークの亀裂事象は，システムレベルである原子炉全体の検証（試験，解析等）で実運用移行前に発見することは困難であったと考えられる．次に，サブシステムレベル（タービン）を検討する．当該事象は，タービンのレベルで想定されるべきであり，タービンの検証で発見されるべきであった．直接原因となった20％低負荷運用に対する十分な検証が行われなかったのは，検証計画に不足があったためであり，遡れば，タービンの設計に対する要求が不足していた可能性が高い．サブシステムの設計要求は，システムレベルの運用コンセプトからフローダウンされるため，システムの運用コンセプトとして，100％負荷運用に加え，20％低負荷運用が行われることが明記されるべきであるが，文書の有無は不明である．仮に，20％低負荷運用がコンセプトに明記されていたとすれば，設計要求に反映し，より詳細な解析を実施して不具合事象に気付くことができた可能性もある．一方で，当時の知見では低負荷時に第12段動翼までランダム振動が及ぶことが認識されていなかったとされていることを考慮すれば，知見不足に原因を求めることになるが，当時米国の原子炉は対策を施していたとする文献もあり[25]，設計要求設定時または設計審査時に，より広範に知見を集めることが必要だったと言える．

以上より，Dual Vee Model による根本原因解析の結果として，運用コンセプトの記述の不足の可能性，知見不足に起因する設計要求の不備，設計審査時の見落とし，サブシステムレベルの試験項目または試験時取得データの不足，を改善すべきプロセスとして抽出することができた．再発防止策としては，運用コンセプトの深化，知識の蓄積，審査の充実を提言することができる．

なお，低出力運転時は，定常運転とは異なる状態であり，ヒューマンエラーの分野でもリスクへの注意が求められている．リーズン[26]は，「原子力業界が低出力での停止状態にともなうリスクを正当に評価し始めたのは，ここ十年のことである．制御室運転員向けの訓練及び手順書は，そのほとんどが通常のフルパワー（100％出力運転時）での緊急事態に対処するためのものである．」と指摘している．今回のケースにおいても，定常運用に加え，試験運用についても，設計の上流において十分な検討が必要であったと言える．

3.2　提案手法の適用範囲

従来，事故の原因としては，運用者エラー，設計過誤，安全への不注意，運用経験不足，不適切な訓練，先進技術の使用による失敗，巨大すぎるシステムに見合わない資金と経営等による説明が行われてきたが，Perrow は，システムそのものに着目した[27]．システムのシーケンスの相互依存性（Interaction）及び結合度による分類である．**Fig.4** に示す Interaction/Coupling Chart において，右側（領域2及び4）に相互依存性の高いシステム，すなわち運用が複雑であるシステムがプロットされている．また，上側（領域1及び2）に結合度が高いシステム，すなわち時間依存性が高く運用時の時間遅れを許容しないようなプロセスを有するシステムがプロットされている．これより，右上（領域2）にプロットされているシステムは，破局的な事故を起こしうるポテンシャルを有する．

筆者らは，Perrow の分類に着想を得て，根本原因解析手法の適用範囲の観点からシステムを分類することを考えた．その際，分類の独立変数として選択したのが，複雑性と運用性である（**Fig.5**）．

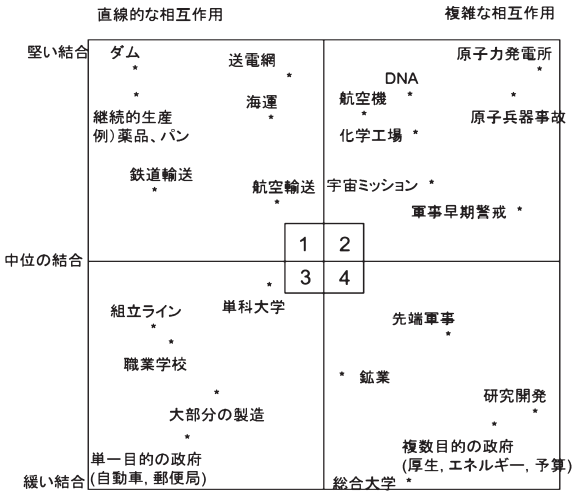

Fig.4　Interaction ／ Coupling Chart[27]を和訳

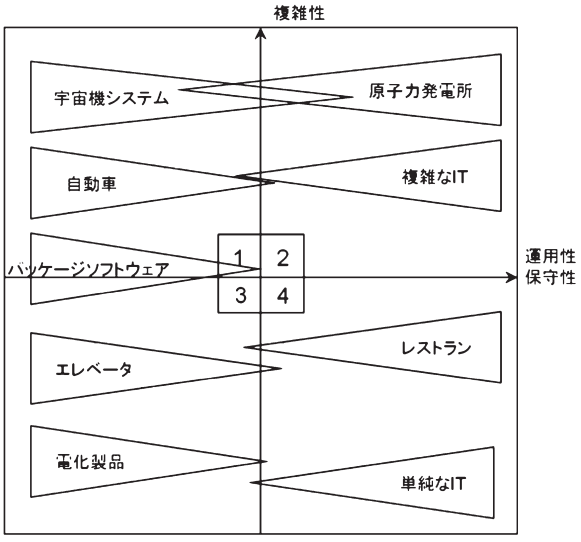

Fig.5　A system chart for root cause analysis tool selection

システムのライフサイクルには種々の表現があるが，**Fig.6** に示す ISO 15288 が代表的である．市場投入を境に，コンセプト段階から製造段階までの開発段階と，利用段階及び維持段階から廃棄段階までの運用段階に大きく二分できる．システムの事故が，開発段階と運用段階のどちらに起因するかを識別することは，根本原因解析を経て組織やプロセスの是正措置を検討するにあたり重要である．複雑なシステムほど開発段階に多くのプロセスを有し，運用段階で発生する事故の原因を作り込む可能性がより高くなると考えられる．よって，システムの複雑性をチャートのひとつの軸とする．また，運用段階において，宇宙機のように運用者の関与が小さいシステムと，原子力発電所のように運用者の関与が大きいシステムが存在し，運用に起因する事故が発生する可能性は大きく異なると考えられる．従って，運用性をチャートのもう一つの軸とする．

ISO 15288：2002

コンセプト段階	開発段階	製造段階	利用段階 維持段階	廃棄段階

NASA

プレフェーズA:コンセプト研究	フェーズA:技術開発	フェーズB:予備設計・技術開発完了	フェーズC:最終設計・製造	フェーズD：システム組立･試験・打上	フェーズE：運用・維持	フェーズF：終結

米国エネルギー省（DoE）

プロジェクト計画段階			プロジェクト実行			ミッション	
プレプロジェクト	プレ概念計画	概念設計	予備設計	最終設計	製造	受領	運用

Fig.6 Generic Life Cycle [29)]

リーズンによれば，主要事故の 80 から 90％がヒューマンエラーによって起こるという考え方が主流になっている [26)]．運用保守の関与が大きいシステムの代表的な例が原子力発電所である．Fig.5 において，原子力発電所は，複雑性及び運用性がともに高い領域 2 にプロットされる．一般的に原子力発電所は，実績のある設計により製造され，長期間にわたり運用されることから，運用保守の関与が大きく，運用に起因する事故が必然的に多くなる．しかし，新規開発された原子力発電所も存在することを考慮すれば，開発段階の不備に起因する事故も発生し得る．三角形を領域 1 に伸ばすことで，数は少ないが，新規開発設備が存在し，開発段階に起因する事故が起こり得ることを表現している．他方，運用保守の関与が大きくないシステムは，人工衛星に代表されるように，必然的に設計製作段階に起因する事故の比率が高くなる．齋藤 [28)] は，公開されている軌道上で発生した衛星の故障に関する情報を分析し，総件数 33 のうち，設計不良及び製造不良が 25 件を占めていることを明らかにした．Fig.5 において，宇宙機システムは，複雑性が高く，運用保守の関与が大きくない，領域 1 にプロットされる．三角形を領域 2 に伸ばすことで，通信衛星のような新規開発要素が少なく，軌道投入後長期間にわたり運用を行うものが存在することを表現している．

原子力発電所や宇宙機システムのような複雑なシステムは，その開発段階でシステムズエンジニアリングの手法を適用する場合が多く，ライフサイクル（Fig.6）を Dual Vee Model で表現できる．したがって，Fig.5 において，領域 1 については，Dual Vee Model を用いた根本原因解析が良好に適用できると考えられる．

4. 考　　察

大規模システムの事故の根本原因解析については，原子力発電所に関する多くの事例が公開されているが，運用や組織に起因するものがほとんどであり，2. 2 に記述した手法を用いて解析が行われている．一方，開発段階に起因する事故に関する報告数は比較的少なく，特定の手法を用いて根本原因解析を実施した事例は見当たらない [18), 22)]．そのような事故に対しては，3. 1 の事例で示したように，筆者らが提案した Dual Vee Model を用いた手法が有効に適用可能である．以下に，従来手法との比較検討を行うことで，提案手法の有効性を考察する．

3. 1. 1 に示した事例 1 については，提案手法を適用した解析結果として，プロダクトを改造する際の設計変更が他の機能性能に影響を与えるかどうかを，さらに上流の機能性能要求に遡って確認，リスクアセスメントを行うことの必要性を指摘した．一方，従来手法により策定された再発防止対策の主要点は，設計の原点に立ち戻ること，及びそれを実現する手段として設計管理指針及び組織を見直すこと，である．両者を比較すると，設計要求に遡って確認することの重要性を指摘している趣旨は同じであるが，従来手法がプロセスを点で捉えているのに対し，提案手法はシステムのアーキテクチャに基づき，設計・要求・コンセプトといったプロセス相互の関係を捉えていることが特徴的である．システムの開発プロセスは，検証計画→検証実施のように相互のつながりを有するものであるため，対策を立案する際には，ひとつのプロセスのみに着目するのではなく，プロセス間の相互関係を捉えることが重要である．

3. 1. 2 に示した事例 2 については，提案手法を適用した結果として，運用コンセプトの記述の不足の可能性，知見不足に起因する設計要求の不備，設計審査時の見落とし，サブシステムレベルの試験項目または試

験時取得データの不足，を改善すべきプロセスとして抽出し，再発防止策として，1）運用コンセプトの深化，2）知識の蓄積，3）審査の充実を提言した．一方，従来手法により策定された再発防止対策は，1）従来知見の適用の妥当性について十分精査した上でモデル試験の適用範囲を決定すること，2）モデル試験計画時に実機を模擬していない項目をリストアップし，開発デザインレビュー等で十分評価すること，3）これらをメーカのタービン設計部門の基準に反映させること，である．両者を比較すると，提案手法は，従来手法の結果をすべて包含し，かつ，従来手法が指定できなかった運用コンセプトの不足の可能性を抽出した点で，より網羅的な解析ができていると言える．

このように，提案手法は，Dual Vee Model をガイダンスとすることで，より網羅的な解析を可能としている．また，必ずしも 3.1 の解析対象システムの詳細が記載されているわけではない公開情報のみをもとに，システムズエンジニアリング的手法を活用することにより，有効な根本原因解析を実施することができた．このことは，提案手法が，解析者の対象システムに対する知識への依存度が低くても実行可能であることを示す．

本論文では，宇宙機及び原子力発電所の事故への適用結果を示したが，Fig.5 に提案した分類チャートにおいて，領域 1 に位置する自動車やパッケージソフトウェアなどのシステムについても，同様に提案手法が有効であると考えられる．

Dual Vee Model を用いた根本原因解析は，不適切なプロセスを識別するものであり，次のフェーズとして，当該プロセスの改善を検討する必要がある．例えば，運用コンセプトの記述不足が明らかとなった場合，同時並行で行われるリスクアセスメントとの双方向フィードバックを活用するなどによって，検証計画の抜けを防止する助けとなる（**Fig.7**）．

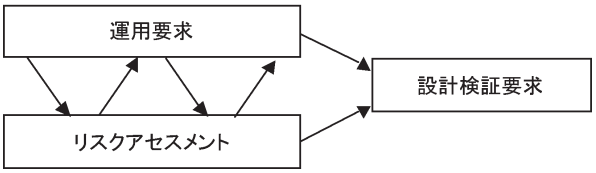

Fig.7　Feedback between Operation Requirement and Risk Assessment

5. ま　と　め

筆者らは，複雑なシステムのひとつである宇宙機システムで発生した事故の根本原因解析を効率的に実施する手法として，Dual Vee Model を適用することを提案し，その有効性を実証してきた．宇宙機システムは，複雑かつ開発段階（設計製作試験）における制約が多く，運用保守の関与が小さい特徴を有する．一方，原子力発電所のシステムは，同様に極めて複雑であるが，運用保守の関与が大きいことが異なる．本論文では，原子力発電所システムの事故の根本原因解析のなかで，システム開発段階に起因するものについては，提案手法が有効であることを，実例をもって示した．さらに，システムを複雑性と運用性の二軸を有するチャートで分類することにより，提案手法が有効である分野を明確にし，宇宙機システムや原子力発電所システムの他にも自動車等の分野にも適用できる可能性を示した．

謝　辞

本研究の実施に当たり，独立行政法人宇宙航空研究開発機構のデータを使用させていただきました．また，慶應義塾大学大学院システムデザイン・マネジメント研究科戦略システムデザインラボのメンバーから有益な助言をいただきました．ここに謝意を表します．

参考文献

1）　Office of Safety　& Mission Assurance, Chief Engineers Office, NASA, Root Cause Analysis Overview（2003）
2）　Andersen, B. and Fagerhaug, T., Root cause analysis, Second Edition, ASQ Quality Press, Milwaukee（2006）
3）　Ohno T., Toyota Production System, Productivity Press, Portland（1988）
4）　Lee W.S., Grosh D.L., Tillman F.A., Lie C.H., Fault Tree Analysis, Methods, and Applications – A Review, IEEE Transactions on Reliability, Vol.R － 34, No.3（1985）
5）　弘津祐子，根本原因分析を活用した安全管理システム，安全工学，Vol.46，No.4（2007）
6）　Fussell J.B., Powers G.J., and Bennetts R.G., Fault Trees – A State of the Art Discussion, IEEE Transactions on Reliability, vol.R-23, No.1（1974）
7）　Maejima, H., Kohtake, N. and Ohkami, Y., A Root Cause Analysis Method using Dual Vee Model for Cause Identification Reliability Improvement, 22nd Annual INCOSE International Symposium（2012）
8）　Forsberg, K. and Mooz, H., The Relationship of System Engineering to the Project Cycle, the joint conference sponsored by：National Council On Systems Engineering（NCOSE）and American Society for Engineering Management（ASEM）
Chattanooga, TN 21-23（1991）
9）　Takano, K., Sawayanagi, K. and Kabetani, T.,Development of Remedy-Oriented Analysis and Evaluation Procedure, Journal of Nuclear Science and Technology, 31［9］, pp.894-913（1994）
10）　NASA Systems Engineering Handbook, NASA/SP-2007-6105, Rev 1
11）　Nagano, S., Program and Management Process, Systems Engineering, Vol.11, No.1（2008）
12）　平成 20 年第 26 回宇宙開発委員会資料

13） H-ⅡAロケット6号機打上げ失敗の原因究明及び今後の対策について，平成16年6月9日，宇宙開発委員会，など
14） Kubota, Y., Takegahara, H., Aoyagi, J. and Kuriki, K., Time-evolutionary method of risk assessment for reliability improvement, IAC-08-D3.4-E5.4.2 (2008)
15） Ishimatsu, T., Leveson, N., Thomas, J., Katahira, M., Miyamoto, Y. and Nakao, H., Modeling and Hazard Analysis using STPA, NASA 2010 IV & V Annual Workshop (2010)
16） Forsberg, K., Mooz, H. and Cotterman, H., Visualizing Project Management, John Wiley & Sons, Inc. (2005)
17） Root Cause Analysis Guidance Document, DOE-NE-STD-1004-92 (1992)
18） Best Practices in the Organization, Management and Conduct of an Effective Investigation of Events at Nuclear Power Plants, IAEA-TECDOC-1600 (2008)
19） Embrey, D.E., Incorporating management and organizational factors into probabilistic safety assessment, Reliability Engineering and System Safety, 38, pp. 199-208 (1992)
20） Ghosh, S.T and Apostolakis, G.E., Organizational Contributions to Nuclear Power Plant Safety, Nuclear Engineering and Technology, vol.37 No.3 (2005)
21） 事業者の根本原因分析実施内容を規制当局が評価するガイドライン，原子力安全・保安院，独立行政法人原子力安全基盤機構，平成22年改定1，p.1
22） 佐藤猛，渡辺憲夫，吉田一雄，原子力研究施設等の事故・故障等に適用した根本原因分析手法，JAEA-Technology 2009-028，pp.2-3
23） 中部電力株式会社浜岡原子力発電所1号機における配管破断事故について（最終報告書），第29回原子力委員会資料第1-2号，平成14年
24） 浜岡原子力発電所5号機タービン振動過大によるタービン自動停止に伴う原子炉自動停止について（低圧タービン第12動翼の損傷），第69回原子力安全委員会資料第2号添付資料2，平成18年
25） 日経ものづくり編，事故の辞典，日経BP社，P.362 (2009)
26） ジェームズ・リーズン著，塩見弘監訳，高野研一，佐相邦英訳，組織事故，日科技連 (1999)
27） Perrow, C., Normal Accidents, Princeton University Press, pp.62-100, (1999)
28） 齋藤宏文，人工衛星の軌道上故障に関する二次分析，日本航空宇宙学会論文集，Vol.59, No.690, pp.190-196, (2011)
29） INCOSE SE Handbook Working Group, INCOSE Systems Engineering Handbook V.3.2.2, INCOSE-TP-2003-002-03.2.2, San Diego (2011)

Root Cause Analysis of Accidents on Large-scale Complex Systems using Dual Vee Model

by Hironori Maejima † *Naohiko Kohtake* †*oshiaki Ohkami* † *and Kenichi Takano* †

Root cause analyses of system failures are important from a viewpoint of prevention of recurrence of the failures and occurrence of similar failures. Five-why Analysis and Fault Tree Analysis are most popular however these analysis results depend on the skill of the analysts strongly because these use brain-storming method. The authors have proposed a root cause analysis method using Dual Vee Model, which has given a guidance in space systems applications to analyze and therefore the result less depends on the skill of the analyst. This paper demonstrates the results of the application of the method to failures of Nuclear Power Plants. This paper also proposes a chart to identify systems to which the method can be applied.

Key words : Root Cause Analysis, Dual Vee Model, Nuclear Power Plant, System, Failure

† Graduate School of System Design and Management, Keio University, 4-1-1 Hiyoshi, Kohoku, Yokohama, 223-2458, Japan
E-mail : hmaejima@z8.keio.jp