GSN 及び ESD モデルを用いたソフトウェア FMEA の提案

Failure mode and effect analysis using Goal Structuring Notation and Event Sequence Diagram for Software

国立研究開発法人　宇宙航空研究開発機構　研究開発部門　第三研究ユニット
(Research and Development Directorate, Japan Aerospace Exploration Agency)
○梅田　浩貴　　波平 晃佑　　祖川 和弘　　植田 泰士　　片平　真史
○Hiroki Umeda　Kohsuke Namihira　Kazuhiro Sogawa　Yasushi Ueda　Masafumi Katahira

Abstract　Failure Modes and Effects Analysis (FMEA) for software-intensive system has difficulty in setting failure modes because software itself never fails and item is abstract. Meanwhile, visibility of expert knowledge is not enough, it is difficult to share idea method of failure mode. In this paper, we will guide the thought process of expert engineers in the analysis framework and explain the technique based on the view of Goal Structuring Notation and Event Sequence Diagram.

1.　はじめに

JAXA では、宇宙機システムのソフトウェア（以下、SW という）を開発する際、要求の抽出や設計レビュー、重要なケースへの試験の網羅性向上、システム限界や制約の抽出のために FMEA（故障モードと影響解析）[1]を行っている。FMEA がそれらの効果を発揮するには、如何に影響が大きな「故障」を網羅的に導出するかが重要であるが、SW に対して FMEA を適用する際、下記の課題が発生していた。

・課題①：分析行為におけるエキスパート依存性の高さ

SW は FMEA を適用する単位（以下、アイテムという）が機能名称等の抽象となるため、SW の「故障」を発想する難易度が高い。広く普及しているハードウェアに対する FEMA では、アイテムが部品・材料であるため、部品・材料の経年劣化等を想起させる汎用的誘導語によって直接的に故障の想起を支援することができる。一方、SW に対する FMEA では、アイテム自体が設計書にある抽象概念であるため、誘導語の適用を行ったとしても具体故障を発想する過程の属人性は高く、分析結果の質は分析者の能力・経験量に依存する（以下、エキスパート依存という）。経験量が低い技術者が発想した場合、SW の動作を含めた故障シナリオにつながらない故障モードとなることがある。また、SW の誤動作は、協調動作等の複数の条件が破綻して非局所的に発生することが少なくないが、そのような故障モードを単一アイテムだけで発想するのは困難であり、エキスパート依存性を高めている。

・課題②：分析結果に対するレビューの困難性

故障によって生じるシステムへの影響は、システムが置かれる状況によって異なるため、システムの利用状況を考慮して分析する必要がある。SW の場合、アイテムの特性によって、考慮すべき影響先も、後続の機器、システム全体、利用者など様々異なる。その影響先の多様性、あるいは前述の非局所的に発生する故障の存在を踏まえると、分析の質を高めるためには多数のステークホルダーのレビューも重要となる。一方で、課題①のエキスパート依存性の高さから、故障モードの導出過程や影響判断根拠などの分析過程の可視性は高くないため、分析結果に対するレビューも困難となる。

・課題③：過去フィールドデータ活用の困難性

宇宙機システムの開発期間は 5 年程度など長期間になることが多く、また JAXA で開発する製品は、研究要素が高く大量生産品ではない。そのため、大量のフィールド情報（不具合情報等）や FMEA の実施機会から誘導語を製品固有に活用・最適化するアプローチをとることが困難であり、如何に長期に様々な開発に従事しているエキスパートの知見を最大限に活用し、少ない開発機会から非エキスパートに技術伝承することが重要となる。

〒305-0081 茨城県つくば市 1 千現 2-1-1　筑波宇宙センター　Tel：050-3362-2805
e-mail:umeda.hiroki@jaxa.jp　Tsukuba Space Center,2-1-1 Sengen Tsukuba,Ibaraki,Japan

2. 手法の前提概念

2.1 ソフトウェア FMEA とその課題

FMEA は、システムにおいて発生する故障を抽出し、その影響の致命度に基づく相対的な定量評価等に基づき、故障に対する対策を検討する手法である。その分析結果の質・効果は、分析対象アイテムの選択と故障の発想が重要であり、SW に対する FMEA（ソフトウェア FMEA）[1]では、アイテムを「機能」として故障の分析することが多い。なお、本論文では「故障」を「アイテムが要求機能達成能力を失うこと」[2]として「異常」や「意図しない動作」も含むものとする。故障の発生過程として、外部からストレスが加わることで故障メカニズムが進行し、最終的に人や機器が故障と認知する。システムの利用時における影響を判断する場合、SW の故障は故障メカニズムの一部を担っている（図 1）。ソフトウェア FMEA では、システムの故障メカニズムに該当する SW の動作を「故障モード」と呼ぶ。

故障の発想を促す仕組みの事例として HAZOP[3]がある。HAZOP は、なし(no)、逆(reverse)、他(other than)、大(more)、小(less)、類(as well as)、部(part of)、早(early)、遅(late)、前(before)、後(after)といった「時間、質、量」の観点からその反対概念を発想させる誘導語を用いて分析者に故障の発想を促している。ソフトウェア FMEA では、アイテムが抽象的であることや、SW は論理単体では故障しなく、複数のアイテムの関連から故障を発想する必要があるため、既存の誘導語を用いた故障の発想方法は、下記の課題がある。

・誘導語がアイテムの特性に合っていない場合、その発想負荷が高くエキスパート依存である。
・技術者の経験が浅い場合、誘導語の範囲しか発想しなくなる。

その解決策の 1 つとして、特定の分野に特化した汎用的なアイテムとその誤り状態をリストとして用意して、故障の発想を促す方法[4]も考案されている。

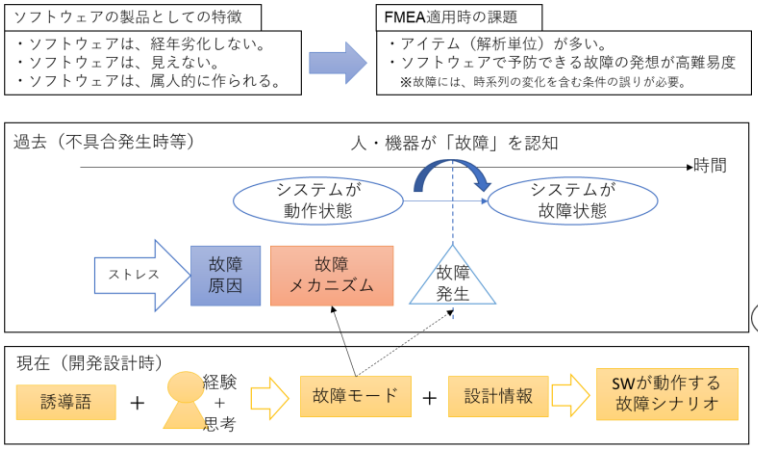

図1：故障に関する概念

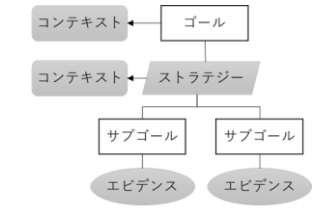

図2：GSNモデリングルール

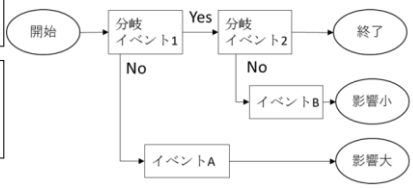

図3：ESDモデリングルール

2.2 GSN（Goal Structuring Notation）とは

GSN[5]とは、ロジックツリーに対し、ゴールの分割視点を表現した「ストラテジー」、ゴールの前提情報を明記した「コンテキスト」、ゴールを達成している事実情報を追加した「エビデンス」のノードを追加した記法である（図 2）。アシュアランスケースの 1 つである D-CASE [6]として記法が拡張されて活用されおり、顧客との合意形成[7]や設計の可視化[8]として使われている事例がある。また、ソフトウェア独立検証及び妥当性確認の活動(IV&V)では、リスクの導出や検証の十分性を可視化する方法として活用している。[9]

2.3 ESD（Event Sequence Diagram）とは

ESD とは、事象の進展をイベントの時系列として表現する記法である。ESD は、重要な分岐点をイベントの発生有無の 2 択で簡潔に表現したフロー図であり、個別のフローは「ユーザ視点のシナリオ」を表現している（図 3）。シナリオの終点に、ユーザやシステム等への影響を表現している。ESD は、シナリオ視点による故障モードの網羅性を確保する方法[10]や、リスク分析者、設計者、運用者等の異なるステークホルダ間におけるコミュニケーションの促進に使われている。[11]

【キーワード】ソフトウェア FMEA、GSN、ESD、エキスパート、技術継承

3. 提案手法

3.1 概要

提案手法は、従来の発想方法に加えてシステムの利用シーンやソフトウェア製品の特徴点を活用することで故障モードの発想を支援する。そのため、エキスパート知見及び不具合から特徴点を抽出する工程、その特徴点から故障モードを発想する工程、故障モードから影響判定を行った工程の 3 工程に専用のビューを設けている。3 つのビューとは、「特徴点抽出部」は構造ビュー、「故障モード発想部」は GSN 形式によるツリービュー、「影響判定部」は ESD 形式による時系列ビューで表現する。

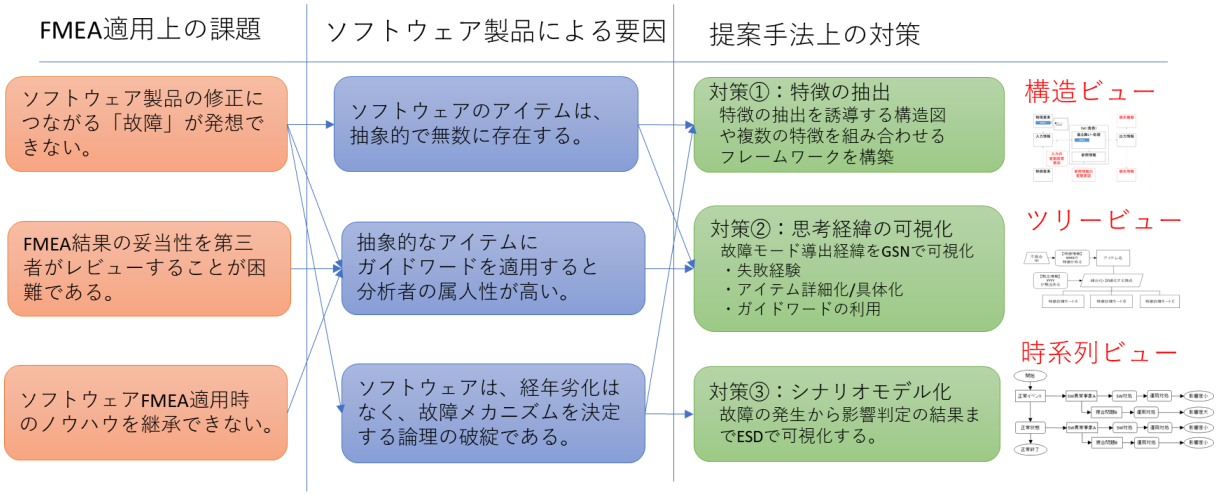

図 4：FMEA 適用課題に対する対策

なお、本論文ではエキスパートの定義は、該当するソフトウェア製品に精通している「製品エキスパート」と FMEA を習熟している「FMEA エキスパート」として、どちらにも習熟してない者を非熟練者とする。分析者のタイプと提案手法が提供する各エキスパートへの期待効果（図 5）は下記である。

①：熟練者への期待効果は、ステークホルダー向けに FMEA 価値の説明（例：SW 仕様が変更されたことで影響度が低くなったシナリオや SW の故障後に対応する運用制約の明確化等）や、熟練者自身の負荷軽減（例：熟練者は故障の発想部分に注力し、非熟練者は故障シナリオによる影響判定を担う）
②：製品エキスパートへの期待効果は、製品開発時と異なる故障の発想方法の提供
③：FMEA エキスパートへの期待効果は、該当製品の仕様を迅速に把握するための特徴点の抽出方法
④：非熟練者への期待効果は、各エキスパートの思考経緯を習得することによる技術継承の促進

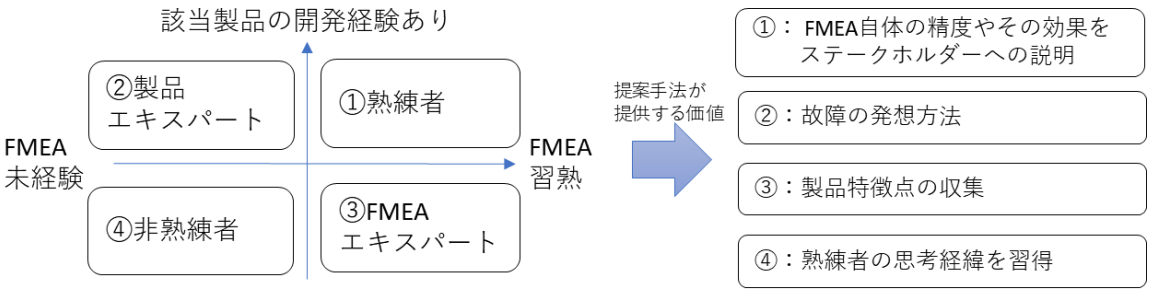

図 5：エキスパート分類と提案手法の期待効果

また、提案手法は、3 つのビューを導入しており、従来の表形式の FMEA に対してモデル化の作業コストが新たに発生してしまう。そのため、一連の分析作業の流れを系統的に実施する分析テンプレートや変換ルールを構築し、GSN や ESD 等の各ビューの生成や、各分析テンプレート間の変換は、ツール(図 6)によって自動変換することで、作業効率化と手法の習得難易度の低下を図った。

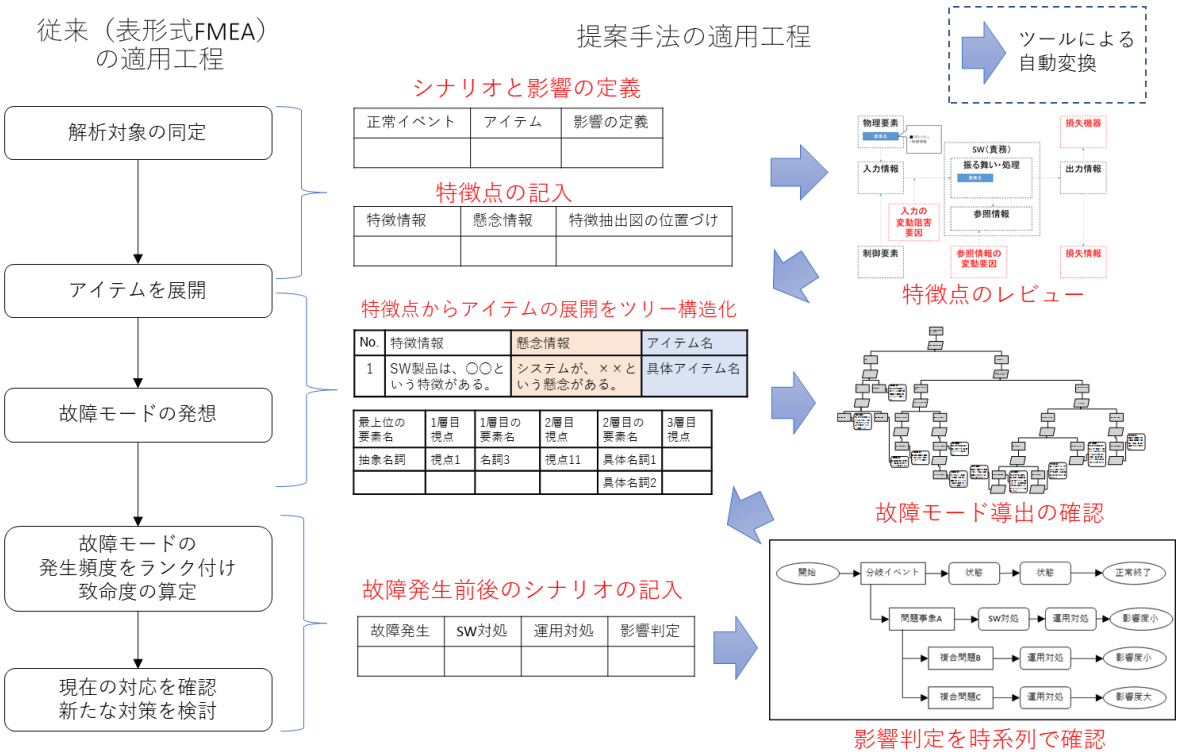

図 6：FMEA 適用工程に対する提案手法の変換ツール概要

3.2　エキスパート知見及び不具合からの特徴点の抽出

エキスパート知見又は不具合情報からアイテムとその特徴点を構造図（図 7：特徴抽出図）で抽出する。特徴点とは、類似アイテムと違いがあり、且つ、ソフトウェアの複雑さを生み出すような仕様のことである。例えば、アイテムが「入力データ」とした場合、「人」と「センサー」からの入力データではその誤り方が異なるため「特徴点」として捉えるが、センサーA とセンサーB のハードウェア故障は SW の入力データの誤り方は同じであるため特徴点として捉えない。一方、センサーの値の意味を考慮すると SW のアルゴリズムで扱いが異なる場合は、特徴点として捉える。このように、どの視点からアイテムを捉えるかによって、抽出される特徴点が変わるため、特徴抽出図の①～⑫の位置付けを参照しながら、アイテムに関連する特徴がないか分析していく。特徴点は故障の発想で活用するため、特徴点から起因する「懸念」があることが必要である。特徴点は SW の役割によって異なるため、より具体的に定義する場合、不具合から同様のアプローチで特徴点を抽出する。なお、故障の発想に活用できる不具合は、単純なバグではなく想定外利用から発生した不具合の方が、より多くの特徴点を抽出できる。

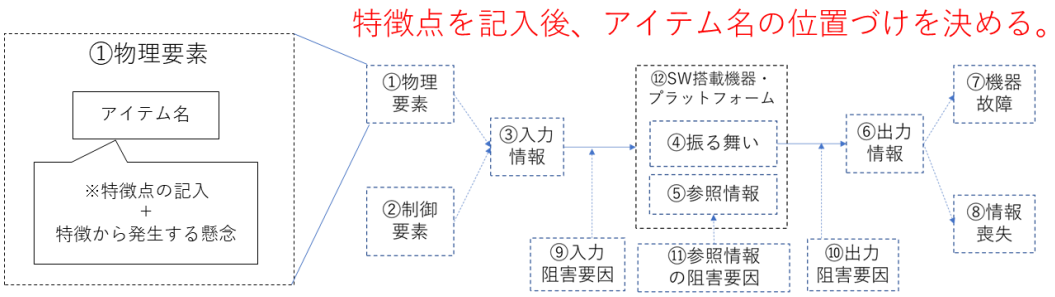

図 7：エキスパート知見および不具合情報から特徴を抽出する図

非熟練者が特徴点から故障モードを発想する場合、特徴点に関連する設計情報を理解することが必要である。そのため、非熟練者が理解すべき設計情報を分析フレームワーク（図 8）で誘導する。特徴点があるアイテムの位置づけ①～⑤によって、収集する情報（どんな状況で、どうして、どうなる、結果こうなる）が異なる点に注意が必要である。

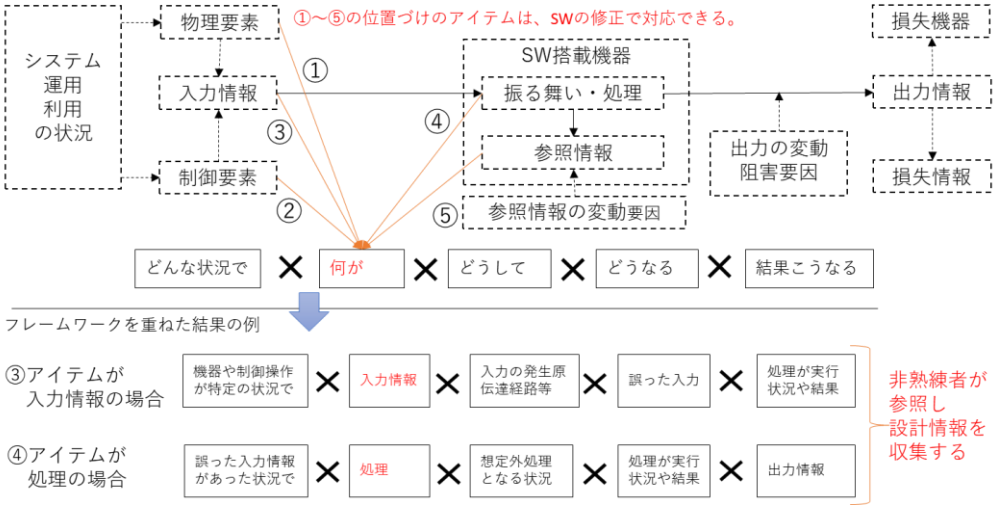

図 8：特徴点から関連する設計情報の理解を促進する分析フレームワーク

FMEA の適用目的が SW の設計や試験のレビューの場合、SW が対応できる故障モードは、SW 自身より以前の①物理、②制御、③入力、④処理、⑤参照情報に位置づけられたアイテムである。

さらに、設計情報の理解を促進しても故障モードの発想が出てこない場合は、HAZOP 等の誘導語を構成する最上位概念「時間、質、量」の視点から該当のアイテム又は特徴点の誤り状態を検討する。SW の場合、アイテム単体では故障を発想できない場合が多いことや、SW の故障は時間を考慮した条件の誤りに誘導していく必要があるので、時間×質、時間×量、質×量といった組合せを 2 軸マトリックスでアイテムの故障モードの発想を促す。なお、本分析は、非熟練者が発想のコツを習得することと、次工程で行う「特徴を参照してアイテムに対して誘導語を設定する」訓練も兼ねている。

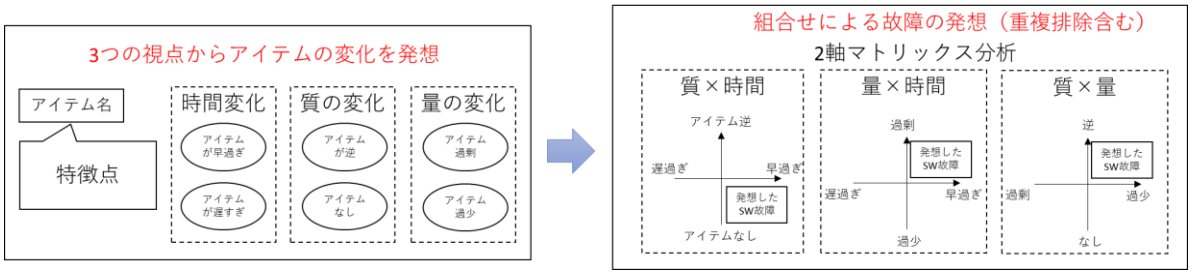

図 9：故障モードの最上位概念からの発想とその組合せ

3.3　故障モードを導出する思考経緯の可視化

一般的に故障モードの発想は、①アイテムの詳細化及び具体化、②失敗経験の活用、③誘導語による発想の 3 つである。その故障モードの発想における導出経緯を表現するため、GSN のモデリングルールは図 10 と定めた。

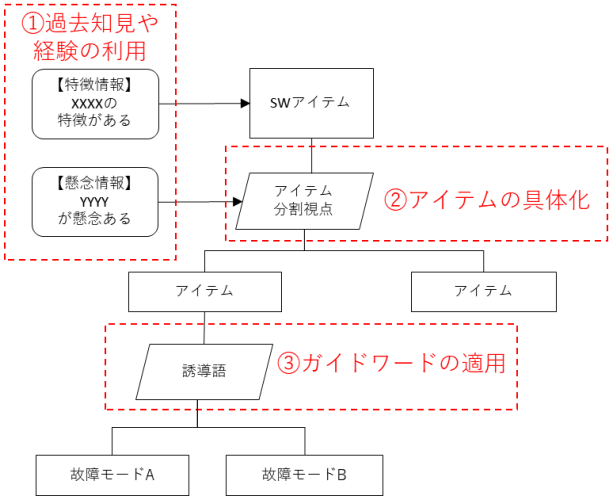

図 10：故障モード導出の GSN モデリングルール

表 1：論理的網羅性のある誘導語例

2 項対立の例	汎用アイテムの分割例
外と内	異常処理（検知、分離、復帰）
開始と停止	異常状態 （継続、停止、一時中止）
連続と単発	冗長化（切り替え前、中、後）
入力と出力	検知処理 （検知、誤検知、未検知）
送信と受信	受信処理（受信、未受信、拒否）
最大と最小	操作（早過ぎ、遅過ぎ、ない）
単一と複数	ファイル処理（過剰、過少、重複上書き、空き・飛び、順序逆）

本手法では、GSN のモデルとしての特徴である、上位下位のゴール（アイテム）は包含関係（具体化）が表現できる、コンテキスト（特徴点）を上位から下位へ継承できる、ストラテジー（アイテムの分割視点）として誘導語の設定もできる、といったことから下記の効果が期待できる。

期待効果①：複数のアイテムを関連付けられることで、複数の特徴の組合せを考慮した故障モードも発想できる。
期待効果②：アイテムの分割視点を論理的な網羅性のある誘導語（表 1）を設定することで、アイテム（仕様）や故障モードの抜けを防ぐことができる。
期待効果③：誘導語の選定が適切でない場合、下位のアイテムに特徴が設定されないため、エキスパートによるフォローが容易になる。
期待効果④：開発の進捗に合わせて、アイテムを具体化しながら故障モードを発想することができる。また、GSN として表現された思考経緯を他の FMEA 実施者やステークホルダーに提示することで、議論の円滑化や合意形成の促進によって、新たな特徴点の抽出され、故障モードの生成できることもある。

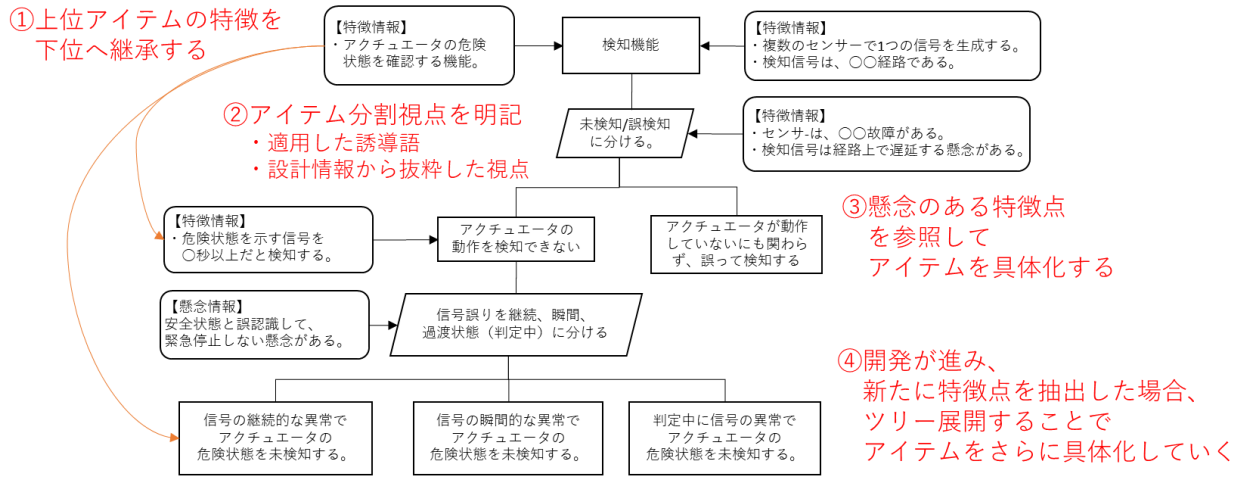

図 11：故障モードの導出経緯

3.4　シナリオビューによる「故障モードの検証」と「故障シナリオの提示」

SW 製品のレビュー等で活用できるのか発想した故障モードを検証するため、故障発生から影響判定までの時系列の推移を ESD としてシナリオモデルで表現する。なお、故障モードのアイテムが抽象的過ぎる場合、シナリオを描くことができず、開発プロセス上で行う検証作業の対策を検討してしまうこともある。（例：入力の誤りは、インターフェース仕様をレビューすることで防ぐ）。その場合は、前工程の特徴抽出や誘導語の適用等を再度行い、アイテムを具体化することで故障モードを修正する。他にも、①故障モードで修正されたシナリオが明確になり FMEA の効果が明確になる、②故障シナリオを利用運用者が確認することでソフトフトウェアからの制約が明確になる、といった効果がある。

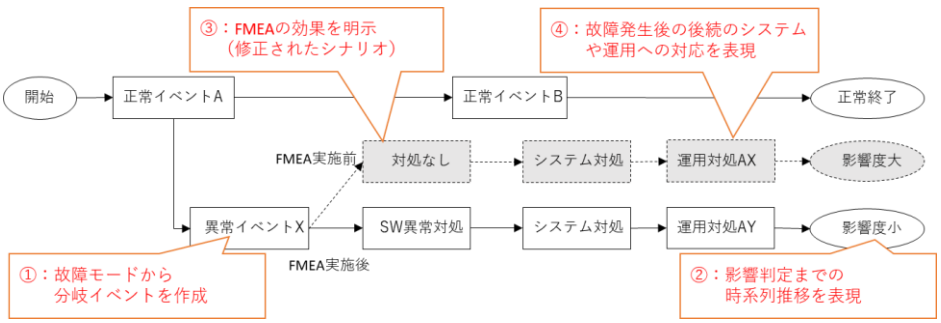

図 12：故障モードから作成した故障シナリオ

4. 提案手法の有効性確認

4.1 有効性確認の方法

提案手法の有効性確認として、下記の 3 つのケース（熟練者、製品エキスパート、非熟練者）を、異なる開発企業で実際の宇宙機システムにおけるソフトウェア開発と並行して適用した。
1 つめの評価指標は、故障の発想が広がっているか確認するため故障モード数とした。2 つめの評価指標は、抽出した故障モードによって仕様修正や試験の追加等の開発フェーズに合わせた FMEA の適用目的を達成しているか、とした。なお、FMEA の適用目的（機能定義、設計レビュー、試験ケースの作成等）は、各組織の開発段階で異なっており、開発と並行して適用し取得できた結果を掲載している。

表 2：実験ケースとその条件

実験 No	提案手法の実施者	対象 ソフトウェア	FMEA 適用目的	評価指標 1 故障モード数	評価指標 2 開発活動への効果
ケース 1 企業 A	非熟練者	組み込み系	試験仕様 レビュー	製品エキスパート との比較	※開発進捗中で今後計測
ケース 2 企業 B	製品エキスパート FMEA 未経験者	組み込み系	試験仕様 レビュー	従来手法（誘導語） との比較	従来の FMEA 実施後に作成した試験ケース数の影響度別の比較
ケース 3 企業 C	熟練者	エンター プライズ系	設計 レビュー	従来手法(不具合分析と経験)との比較	従来の FMEA 実施後に、提案手法で新たな仕様修正を検出できたか。

4.2 有効性の確認結果

3 つの開発組織で行った有効性の確認結果を表 3 から 5 に示す。

表 3:実験結果一覧

実験 No	評価指標	従来手法	提案手法
ケース 1：非熟練者	発想した故障モード数	27	48
ケース 2：製品エキスパート 且つ FMEA 未経験者	発想した故障モード数	31	71
ケース 3：熟練者	発想した故障モード数	12	54

表 4：実験結果一覧(FMEA 未経験者)

実験 No	評価指標（故障シナリオ数）	従来手法	提案手法
ケース 1：非熟練者	故障シナリオ数	14	21
ケース 2： 製品エキスパート 且つ FMEA 未経験者	影響度大（システムへの影響）	91	145
	影響度中（出力先機器への影響）	16	39
	影響度小（一過性の影響）	4	49

表 5：実験結果一覧（FMEA 経験者）

実験 No	評価指標	従来手法	提案手法
ケース 3：熟練者	1 故障モードあたりの FEMA 適用時間 （対策の検討完了まで総時間）	0.46(h)	0.47(h)
	修正件数（仕様や運用制約） ※従来手法後に提案手法を実施	23	11

4.3 考察

非熟練者、エキスパート、熟練者のいずれのケースでも特徴点を用いた提案手法の方が、故障モードの発想数が高くなっている（表 3)。

ケース 1 では、製品エキスパートの経験による故障の発想よりも、非熟練者による提案手法の方が故障の発想が広がっている。しかし、表 3 と表 4 を比較すると、該当製品のレビューに使える有効な

故障モード（故障シナリオ数）の発想効率は非熟練者よりも製品エキスパートの方が高い。これは、非熟練者の場合、製品の特徴点を抽出できず、誘導語による論理的な網羅性を確保することに注力したことが原因である。論理的な網羅性を確保することによる安心感も重要ではあるが、無数のアイテムを属人的に設定できるソフトウェア FMEA では、故障シナリオを抽出できるアイテムを設定できる効率も重要である。そのため、非熟練者が故障モードを発想する場合、製品エキスパートのレビューは、故障モードの導出経緯ではなく、特徴点の抽出後にレビューをすることで適用効率が上がると考えられる。

ケース 2 では、従来手法とした誘導語による発想では、特に「アルゴリズム・処理」のアイテム単体で、ほとんど故障の発想が広がらず、提案手法の方が 2 倍以上の故障モードが定義できている。一方、評価指標 2 では、提案手法で検出できていない試験ケースがあった。提案手法では正常シナリオを設定して分析を行ったため、異常状態における異常入力があった場合の試験ケースが検出できていない。ESD 化した故障シナリオに対して、再度、提案手法を適用することで該当する試験ケースは抽出できるため、今後、手法の改善が必要である。

ケース 3 は、既に表形式の FMEA は実施済であったため、提案手法で新たに故障モードを発想し、その故障モードが設計レビューで効果があるか計測し、一定の効果があったことを示している（表 5)。

時間効率については、FMEA 未経験者の場合、FMEA 自体の習得コストが計上されてしまうため、FMEA の経験者である熟練者のみ計測した。時間計測の結果、分析テンプレートと専用ツールの導入によって、GSN や ESD 等のモデル化作業が加わったとしても従来の表形式と同等の工数となっている（表 5)。但し、抽出する故障モード数も増えているため、従来の開発工数よりも増えるため、さらなる効率化が必要である。

5. まとめ

SW に FMEA を適用する際、そのアイテムが抽象的であるため「故障」の発想が広がらない、一方、アイテムや誘導語を具体化し過ぎると狭い範囲でしか故障を考えられず、上位システムへ影響のある「故障」を考えられない、といった課題に対して、分析フレームワークで誘導し特徴点を抽出、その後 GSN のビューで故障モードを発想、ESD のビューで故障モードの有効性確認することで効果は出ている。
今後の発展として、FMEA は開発の進捗に合わせて繰り返し適用していくことでより効果を出すことができるため、開発工程に合わせて GSN や ESD モデルを繰り返し更新する仕組みと、他の製品に FMEA を適用する際、エキスパートの思考経緯を含めた故障モードの再利用方法が必要である。他にも、よりエキスパートの知見を可視化するためには、故障の発生後や非定常状態である故障シナリオに対し、2 つ目の故障が発生する「複合異常」に対応する必要がある。

6. 参考文献

[1] 新 FMEA 技法, 益田昭彦, 河北印刷株式会社
[2] JIS Z 8115:2000
[3] IEC 61882: Hazard and operability studies (HAZOP studies)
[4] Hisashi Yomiya, 不具合リスク発想のための観点の抽出方方とその効果, SQiP2016
[5] GSN COMMUNITY STANDARD VERSION 1 (http://www.goalstructuringnotation.info/)
[6] Matsuno Yutaka, Takai Toshinori, Yamamoto Shuichiro, D-Case 入門
[7] Mori Motoko D-Case 導入によるシミュレーションＳ／Ｗの期待結果明確化と合意形成, Software Quality Symposium 2014 年
[8] Kobayashi,IoT 時代に求められるセーフティ設計の見える化とは～ GSN 入門～ (http://sec.ipa.go.jp/seminar/20150730.html) 2015 年
[9] JAXA, IV&V ガイドブック～導入編～、～実践偏～ ver1.2 2017 年
[10] ロケットエンジンにおけるモデルベース信頼性評価技術の構築と試行, 先進的な設計・検証技術の適用事例報告書 2015 年度版 事例 15-A-18
[11] Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, NASA/SP-2011-3421,p53