

# 階層的故障分類法による設備保全情報の共有化 —事故や故障の防止を目的とした設備の評価と改善の方策—

萩原 正弥

2011年3月11日の東日本大震災では、M9.0の巨大地震による津波によって、原子力発電所の冷却用電源が喪失し、炉心溶解、水素爆発を含む放射線汚染物質の大気中への放出、汚染水の流出など、大きな被害が発生し、その完全な終息には、まだ多くの時間が必要であろう。筆者の専門分野は“機械要素”で、長年にわたってねじ締結の信頼性向上に関する研究を続けているが、本学生産システム工学科在職以来、設備管理に関する研究にも参加し、製造現場における効率的な保全管理の実現に向けた取り組みを行ってきた。本稿では、設備管理に関する一連の研究活動の中で提案した階層的故障分類法という故障表現方法について説明し、それによって故障や事故による損害を最小化しようとする試みについて紹介させていただく。

## 1 設備保全情報管理の意義

生産や製造現場においては、設備の状態を維持管理する保全活動が不可欠であり、多くの企業では、保全担当部署がその管理に当たっているが、時折、計画外の設備故障が起これ、緊急保全（Emergency maintenance）と呼ばれる活動が行われる（例えば、池田・萩原・中村，1994）。緊急保全では、的確な情報分析（判断）とすみやかな回復作業の実行が重要であるが、その成否や適否は作業に当るクルーの経験や勘に依存するところが大い。理想的に言えば、想定し得るすべての不具合事象について、事前にそれらへの最適な対処方法を決めておくべきであるが、現実には不可能であろう。そこで重要となるのは、過去に起きた事故や故障の経験をもとに、再発防止策を検討し、そこで得られた情報を共有できる仕組みを整備しておくことである。

## 2 設備保全情報の種類と共有化の要点

設備保全の対象は、工場、設備又はその一部に発生する不具合事象、すなわち故障（Failure）であり、共有化すべき具体的な設備保全情報は、以下のように整理できる（萩原，2002）：

- ① 故障の認識・特定に関連する情報
  - 故障の発生箇所（アイテム及び部位）
  - 故障の状態（内容、形態）
  - 故障探索の技術（方法、機器、メカニズム）
  - 故障検出の技術（方法、機器、適用の条件）
- ② 保全作業の計画・実施に関連する情報
  - 故障の程度（影響、被害度）
  - 故障発現の形態（発生時期、発現の特徴）
  - 故障アイテムへの接近技術（方法、機器、手順）
  - 故障の除去・修正技術（方法、機器、手順）

情報の収集・管理（共有化）にあたっては、客観性が最も重要な要素であり、そのためにはデータの“標準化（Standardization）”が必要である。2000年に改正・発効されたJIS Z 8115 [ディペンダビリティ（信頼性用語）]では、原国際規格であるIEC 60050 (191): 1990の内容をもとに、信頼性や保全性評価に関係する多くの用語が標準化されており、その中には、上述の情報の元となる“フォールト”（Fault＝故障の状態）の概念も含まれている。これらは、実際の現場で発生する故障を分類・整理するのに大きな助けとなるが、単にそれだけでは、上述の具体的な情報の標準化には繋がらない。次節以降で述べる“階層的故障分類法”（HFC: Hierarchical Fault Classification）は、このような問題解決の一方法として提案されたものである（Hagiwara, 1996；萩原，1997など）。

## 3 階層的故障分類法

### 3.1 階層的故障分類法 の概念としくみ

図1に、階層的故障分類法 の概念を示す。この方法は、元々、生産工場における設備管理の効率化を念頭において提案されたもので、故障を生産システム（工場）の階層レベルと対比させて表現しようとする点にその特徴がある。工場（工程）の構成要素は、設備、ユニット、アセンブリ、部品などであり、階層には、その上位に“社会”，下位に部品などの不具合を発生させる直接原因としての“ストレス”及びストレスを発生させる元となる“共通原因”レベルが定義されている（萩原，1999）。

階層的故障分類法では、一連の不具合（故障）を階層レベル間の故障モード（Fault mode）の繋がりと表現する。一般に、故

障は“アイテム (Item) が規定の機能を失うこと”と定義されており、各階層レベルには、それぞれ表1のように、アイテムと規定の機能が定義されている。例えば、製品の不良が発生するのは工場が“故障”し、その機能である良品の生産ができないからであり、それが社会レベルの故障である環境悪化や生命の危機に繋がることもある。また、その原因は、工程を構成するいずれかの設備の故障であり、その原因を作った部品またはユニットの故障は設計ミスや作業ミスによって起こされたものかも知れない。このように、階層的故障分類法では、ある不具合に関し、その原因から最終的な影響に至る“経路”を階層レベルごとに明示することによって、設計段階での事前の検討や再発防止のための情報を得ることを目的としている。

表2は、システムの信頼性評価手法として、従来から用いられているFMEA/FMECA (Failure mode and effects analysis/ Failure mode, effects and criticality analysis) 及びFTA (Fault tree analysis) と、階層的故障分類法の特徴を対比して示したものである。

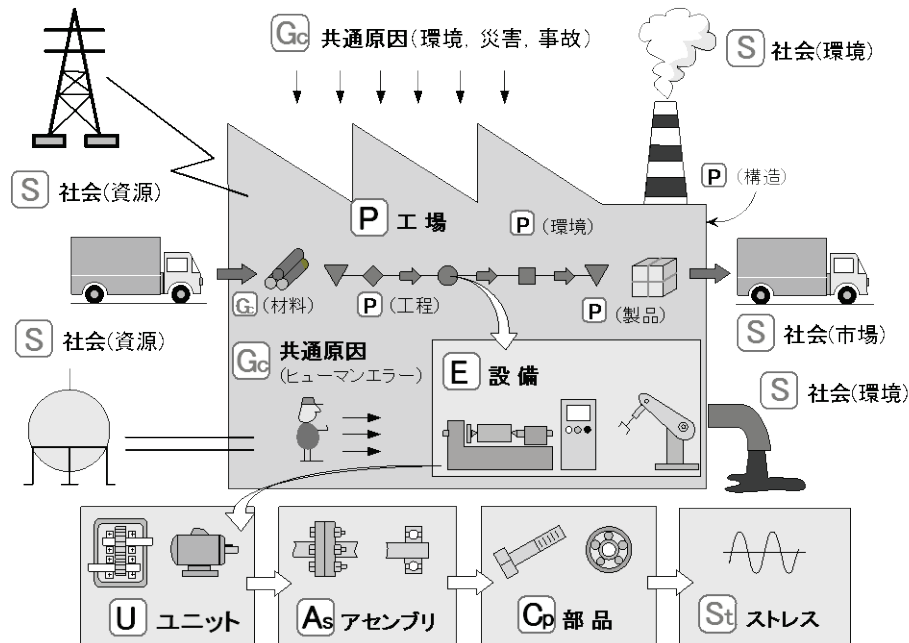


図1 階層的故障分類法の概念—階層レベルと故障モードの繋がり

表1 階層的故障分類法における故障の定義 (萩原, 2002に加筆修正)

故障レベル	アイテム	規定の機能	分類の基準[従来の分類名]
I	社会(S)	人類・生物	致命度 [critical/ non-critical] 被害・損害の大きさ [major/ minor]
		自然	
	工場(P)	工程 (設備群)	
		基盤構造	
II	設備(E)	設備	発生形態 [intermittent/ permanent] [determinate/ indeterminate] 程度 [partial/ complete]
	ユニット(U)	機能ユニット	
III	アセンブリ(As)	部品の組合せ	モード及びメカニズムに依存した個別の故障名称
	部品(Cp)	部品	
IV	ストレス(St)	材料 (分子構造)	原因 [misuse/ mishandling/ weakness/ design/ manufacturing/ ageing]
	共通原因(Gc)	工場人員	
		基盤構造	

表2 故障アセスメント手法の比較

手 法	FMEA/FMECA	FTA	階層的故障分類法(HFC)
目 的	a. 影響による故障のランク付け b. 保全又は設計変更のための情報支援	a. 好ましくない事象に対する原因及び条件の詳細な検討 b. 信頼度解析	a. 故障及び故障間の相互関係の明確化 b. 保全又は設計変更のための情報支援
解析・評価の対象	システム全般 (単一の故障)	システム全般 (単一の頂上事象)	生産システム／一般のシステム (単一の故障／故障系列)
解析・評価の方向	ボトムアップ (原因⇒影響)	トップダウン (事象⇒原因)	両方向 (現象⇔現象)
評価内容	定性的	定性的／定量的	定性的
実施時期	設計（運用）の段階	設計の段階	運用（設計）の段階
特 長	ワークシートによる作業の簡便性と汎用性	論理ゲート（故障の木）による正確な表現	階層構造による客観的／体系的情報管理

この表から、階層的故障分類法（HFC）は、FMEAとFTAの中間的な特徴をもっていることが理解されよう。この方法の具体的な活用事例については、第4節で述べる。

### 3.2 階層的故障分類法の体系

表1の右欄には、各階層レベルに対する故障分類の基準が示してあり、さらに括弧書きでIEC 60050 (191)の故障（Fault）の名称を対応させている。この表から、階層的故障分類法における故障の表現には、現象や状態を表す“フォールト”が用いられており、JIS Z 8115に定義・分類されているさまざまな種類の故障は、階層レベルと対比させることによって初めて意味をもつことが理解されよう。

表3は、表1の分類基準に基づいて作成した故障分類の体系である。FMEA/FMECAでは、工場や社会に及ぼす影響度をもとに故障の評価を行い、それによって事前又は事後の（保全）対策を決定しようという目的があるが、実際の現場では「どんな内容の保全をいつ実施するか」という具体的な問題に対する答えも重要である。階層的故障分類法では、現場で起こる故障による一連の不具合を共通原因レベルから社会レベルに至る故障モードの繋がりで表現するため、保全は「その波及経路をどのレベル（場所）で遮断するか」という具体的な問題に置き換えて考えることができる。表3に示されている“CBM政策”は、故障の波及を止めるレベル、すなわち上述の保全の実施レベルを表している。“CBM”とは、状態基準保全（Condition Based Maintenance）のことであるが、これは、保全を実施するために、そのレベルの故障モード、すなわち故障の状態を監視し、その状態を基に保全を行うことが必要だからである。従来の保全の区分（さまざまな保全の名称分類）は、すべて“〇〇レベルの状態基準保全”と言い換えることができる。例えば、予防保全と事後保全の区別は、ストレスレベル（St）での保全実行の有無を、状態監視（基準）保全とは、部品レベル（Cp）又はアセンブリレベル（As）での故障状態の進展に基づく保全実行の有無をそれぞれ表しており、保全予防（Proactive maintenance）や設計段階での評価・改善は、共通原因レベル（Gc）での状態基準保全であるということができる。

## 4 階層的故障分類法による故障・事故アセスメントの例

### 4.1 スリーマイル島原発事故～福島第1原発事故の分析

図2は、階層的故障分類法の原理にしたがって描いたスリーマイル島原発事故の記述である。1979年3月に起こったこの事故は、最も複雑な複合故障の例として知られている。複合故障（Combined failure/ Dependent failure）とは、複数の故障原因が同時に作用して起こる故障や、他の故障によって誘発されたストレスが新たな故障（二次故障）を起こすような故障の連鎖である（例えば Villemeur, 1992）。図中に記されたANDゲートが前者を、上位レベルから下位レベル又は同一レベルに繋がる矢印（実際には、すべてストレスレベルの故障モードを経由）が後者（二次故障）を表している。また図に“命令（コマンド）”とあるのは、例えば停止信号などの命令（コマンド）によって機器が停止したような状況を表しており、誤った信号や、信号による誤動作以外は故障ではなく、単なる状態の変化を表している。

3.2で述べたように、上位レベルへの故障の波及を止めるためには、そこへ繋がる経路を遮断すればよい。試みに、故障の元となった共通原因故障（この場合は3種類のヒューマンエラー）のいずれかが起こらなかったと仮定し、そこからの経路（矢印）を切断してみたい。図に残された経路を辿ってみれば、そのことによって炉心熔融などの上位レベルの故障現象が発現しなかったことが理解できるであろう。

表3 階層的故障分類の体系 (萩原, 1999)

故障レベル		故障モード(コード)				CBM政策	共通原因故障の分類
		区 分	状 態				
I	社 会(S) Society		非致命的		致命的	P	<div>■ ヒューマンエラー</div> <div><input type="checkbox"/>操作のエラー GcMO</div> <div><input type="checkbox"/>保全のエラー GcMR</div> <div><input type="checkbox"/>検査のエラー GcMI</div> <div><input type="checkbox"/>管理のエラー GcMA</div> <div>■ アイテムの欠点</div> <div><input type="checkbox"/>設計上の欠点 GcWD</div> <div><input type="checkbox"/>製造上の欠点 GcWM</div> <div><input type="checkbox"/>自然の劣化 GcWW</div> <div>■ 自然環境</div> <div><input type="checkbox"/>温度 GcNT</div> <div><input type="checkbox"/>気圧 GcNP</div> <div><input type="checkbox"/>湿度 GcNH</div> <div><input type="checkbox"/>振動 GcNV</div> <div><input type="checkbox"/>腐食 GcNC</div> <div><input type="checkbox"/>塵芥 GcND</div> <div><input type="checkbox"/>その他 GcNO</div> <div>■ 災害・事故</div> <div><input type="checkbox"/>地震 GcAE</div> <div><input type="checkbox"/>落雷 GcAT</div> <div><input type="checkbox"/>水害 GcAW</div> <div><input type="checkbox"/>風害 GcAS</div> <div><input type="checkbox"/>火事 GcAF</div> <div><input type="checkbox"/>その他の事故 GcAO</div>
		広域的	SGNc		SGCr		
		局所的	SLNc		SLCr		
	工 場(P) Plant		軽度	重度	致命的	E	
		製品	PPMi	PPMj	PPCr		
		工程(ライン)	PLMi	PLMj	PLCr		
		環境	PEMi	PEMj	PECr		
II	設 備(E) Equipment		間欠的		永続的	U	
		製造設備	EPdI		EPdP		
		輸送設備	ETpI		ETpP		
		貯蔵設備	ESiI		ESiP		
		検査設備	EIpI		EIpP		
		補給設備	EUtI		EUtP		
	ユニット(U) Unit	動力系	UPwI		UPwP	As	
		伝達系	UTmI		UTmP		
		作業系	UOpI		UOpP		
		制御系	UCtI		UCtP		
		検出系	UDtI		UDtP		
III	アセンブリ(As) Assembly	機械的結合	AsMI		AsMP	Cp	
		非機械的結合	AsNI		AsNP		
	部 品(Cp) Component	故障メカニズムによる分類				St	
		機械部品	CpMX				
		非固体部品	CpNX				
		電気部品	CpEX				
		信号・情報	CpSX				
IV	ストレス(St) Stress		静 的	動 的		Gc	
		機械的負荷	StMS	StMD			
		化学的負荷	StCS	StND			
		電氣的負荷	StES	StED			
		熱的負荷	StTS	StTD			
	共通原因(Gc) Generic cause	右欄参照					

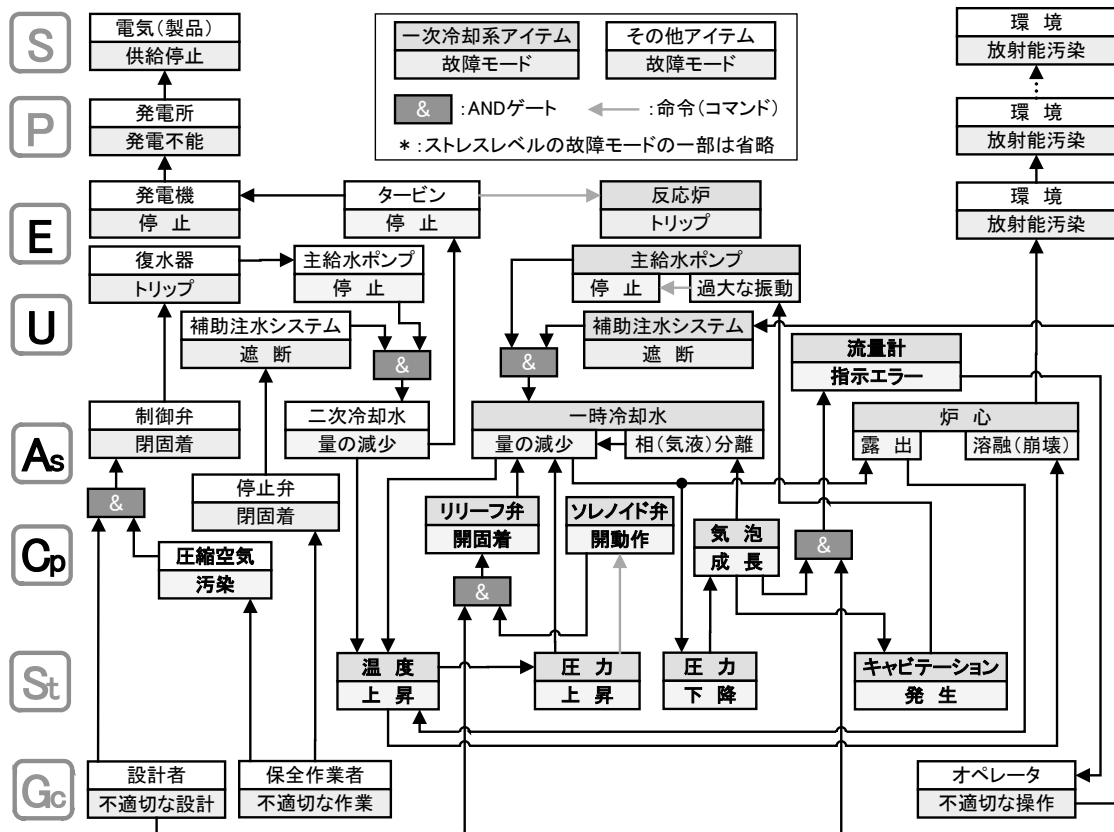


図2 スリーマイル島原発事故の解析例 (Hagiwara, 1996 ; 萩原, 1997)

一方、先の福島第1原子力発電所の事故ではどうだったであろうか？筆者の手許には詳細な情報がなく、また本稿執筆時点（2011年5月）ではまだ作業が継続中であるため、解析図を提示するのは後日とさせていただくが、この場合の共通原因は自然災害（津波）であった。このような場合、同時並行的に故障が発生・波及することが問題で、今回は、電源喪失（停電＝電気のストレス）によるモータ、ポンプ類の停止と非常用ディーゼル発電設備の停止に端を発し、熱的ストレス（温度上昇）から起こった機械的ストレス（圧力増加）と化学的ストレス（水素発生）による二次故障が上位レベルの故障へと繋がっている。共通原因故障への対処が重要なのは、それが一連の故障の“元”であることのほかに、“共通”の名前のとおり、それが同時並行的かつ広範囲に上位レベルに波及するおそれがあることによる。特に自然災害では、複数系列の安全対策を施していたとしても、その規模（発生するストレスの大きさとその範囲）によっては、全ての系列に被害が及んでしまうため、想定したレベルでの保全が成功しない状況を想定しておく必要がある。特に原子力発電所のように、致命度が高い事象を含むケースでは、その故障の波及を防止するような二重、三重の対策が必要となる。

その際、重要となるのは、保全レベルの考え方である。一般に、より下位レベルでの保全を実施することによって被害や損害は最小化できるが、技術的な難度が高く、それを実現するために専用の機器や設備が必要となり、余分なコストが発生するだけでなく、“失敗”の確率が増加する傾向にある。反対に上位レベルで保全を行うことは、被害（損失）の拡大に繋がるが、技術的な要求レベルは低くて済む場合が多い。システムの保全レベルを決める際の基準の一つは、FMECAで言う“Criticality”，すなわち致命度×発生（予想）確率である。今ここで、その具体的な数値の基準を示すことはできないが、何百年に一度起こるかも知れない自然災害を想定し、それに対して、ユニットレベルや設備レベルで完結できるような保全政策を計画し、実行することは、必ずしも得策とは考えられない。一方、百年に一度の大きな災害が、明日起こらないとも限らないのが現実である。重要なのは、故障モードが工場レベルを超えて、社会レベルに波及するような事態を“想定”し、2次、3次の対応策（防止策）を事前に検討しておくことである。これらの対策は、必ずしも専用の設備や機器の直接的な配備（常設）を意味していない。若干変な例かも知れないが、山火事が起こったとき、周囲に溝を掘り、民家への類焼を食い止めるような考え方である。大事なことは、最悪の事態への対応方策を事前に検討しておくことによって、速やかな意思決定が行われ、対応の時間遅れを最小化することである。状況をもとに適切な場所を決め、瞬時に実行に移さなければ、その効果は期待できない。結果として、それが被害の拡大に繋がる。今回の福島原発事故では、このことに対する“備え”に問題があったのかも知れない。

#### 4.2 生産現場での活用事例

前述の例は、事故原因の探索と再発防止策の検討を目的としたものであったが、ここでは、もう少し身近な例を用いて、本来の目的である生産現場での保全政策決定のための活用方法について述べることにする。

図3は、ある部品製造工場における、設備故障解析（故障アセスメント）事例である。この例では、最初に作業者が円筒研削盤の異常音と加工面の不良（びびり）を発見し、そこから下位レベル方向の原因探索と上位レベル方向の影響評価が実施されている。それぞれの故障モードには、それを認識するのに最も適した状態監視方法、又はその排除のための方策が記入されている。この場合、最終的に、故障の元となった潤滑油の種類を変更し、さらに玉軸受の損傷をFFTを利用して監視して設備を停止するという改善（改良）が行われたが、4.1で述べたように、どの保全レベルを選択するかによって、当然対策の内容や意味も大きく異なってくる。極端な例を挙げれば、出荷段階で製品を全数検査（工場レベルの状態基準保全）し、不良品を選別すれば、作業者の監視は不要であり、製品不良によるリコールも回避できることになる。また、軸受寿命を計算によって求め、それにしたがって軸受の交換（ストレスレベルの状態基準保全）を行えば、設備の不具合が防止でき、不良品は発生しないことになる。実際には、前者では製造コストの極端な増加から、後者では、寿命に対する推定精度の問題で技術的に不可能と判定された。

この例からわかるように、階層的故障分類法の特徴は、故障の記述に階層レベルという絶対座標軸が設定されていることである。最初に認識される故障のレベルは、作業者の経験や現場の状況によってさまざまであろうが、そこから作り出される故障の情報（故障系列）は、最終的に同じものになり、このことが評価の客観性を担保している。その手順は、以下のように要約できる：

1. 認識された故障モードの記述（レベル及び内容）
2. 故障モード系列の作成（原因探索及び影響評価）
3. 各故障モードに対する検知・除去技術（保全政策候補）の記入
4. 故障分類（表3）、並びに損害、コスト及び技術的制約にもとづく各保全政策の評価
5. 最適保全政策の決定・実施

十分な知識や経験のある専門家にとっては、このような手順は冗長に感じられるかもしれないが、得られた情報を、表3のような“抽斗（ひきだし）”に格納し、それらを蓄積してさらなる知識として活用することが情報共有化の第一歩であり、それが故障や事故の損害を最小化することに繋がることになる。

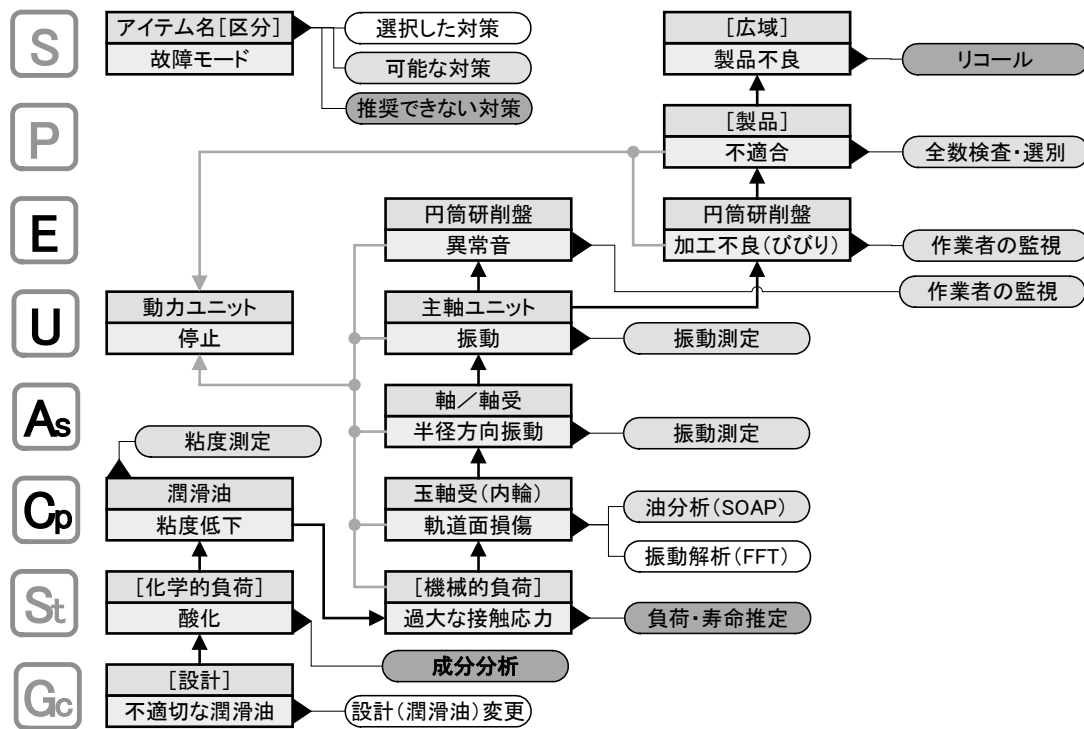


図3 製造工場における故障アセスメントの例(Hagiwara, 2010)

## 5 あとがき

設備保全の体系化を目指した取り組みとして、階層的故障分類法の考え方、及びそれによる故障・事故アセスメントの活用事例について紹介させていただいた。筆者はかなり以前から、この考え方を利用して、インターネットによって故障診断のためのメンテナンス技術データを一般に提供する仕組みを構築しようと構想し、そのためのデータベースの構造や用語の標準化の問題や実際のデータ管理の仕組み（運用方法）について継続して研究や検討を行っているところであるが、残念ながら、まだ実現には至っていない。この件に関しては、あらためてご報告させていただくこととして、本稿が、少しでも読者諸兄の参考になれば幸いである。

## 参考文献

- Hagiwara, M., A New Technique in Maintenance Management based on Hierarchical Fault Classification, *Advances in Industrial Engineering Applications and Practice I*, International Journal of Industrial Engineering – Applications and Practice, Cincinnati, OH, 1996, 1060-1065.
- Hagiwara, M., Chapter 11: Maintenance Data Management: Acquiring and Creating Knowledge for Maintenance Activities, Mital, A. & Pennathur, A. ed., *Industrial Resource Utilization and Productivity*, Momentum Press, 2010, 191-204.
- Villemeur, A., *Reliability, Maintainability and Safety Assessment, Volume 2: Assessment, Hardware, Software and Human Factors*, John Wiley & Sons, 1992, 368-404.
- 萩原正弥「階層的故障分類に基づく設備診断の体系」設備診断技術体系化ガイドブック編集委員会編『設備診断技術体系化のためのガイドブック』日本プラントメンテナンス協会, 1997, 27-38.
- 池田良夫, 萩原正弥, 中村雅章『設備管理 生産管理—理論と実践7』日刊工業新聞社, 1994, 6-9.
- 萩原正弥「メンテナンスデータの共有化技術」『精密工学会誌』65 (3), 1999, 377-380.
- 萩原正弥「メンテナンス・データの構造と標準化」『日本設備管理学会誌』14 (1), 2002, 29-34.
- 柳田邦男『恐怖の2時間18分』文藝春秋, 1983 ; 同 文春文庫, 1986.