

機械安全における確定的 F T A [H E F T A] の提案

Deterministic FTA Method based Hazard and Exposure: HEFTA Analysis

安全技術応用研究会 (S O S T A P) 会員

○ 石原立憲¹⁾

杉浦 澄²⁾

Even FTA is used also for the industrial work injury analysis, it is likely to become a diffusion system, and doesn't reach the root cause of event easily, and probability data of occurrence of each factor is very few. In our country additionally, it is very likely to be concluding easily that so-called "Human error" from incompleteness of the education and training are the cause of event. Such situations very often make the root causes and effective prevention measures not be logically extracted and judged. While, if the hazard energy doesn't exist or lower than the level that the worker is injured, or if he does not come in contact with the hazard energy, the risk of the industrial work injury could not be generated determinately. Then, it is reported here combining the "Deterministic risk assessment" logic by, risk = binary of presence of Hazard × binary presence of Exposure, with the priority level of the evaluation method and the safety measures by the international safety standard, "Deterministic FTA :HEFTA analysis" that is able to fix a root causes and determine prevention measures in the work injuries easily by everyone is designed.

1. 報告の狙い

問題事象の要因をトップダウン的に抽出する F T A (Fault Tree Analysis) は、生産現場の労働災害分析にも使用されているが、下記の問題を持っている。

- ① F T A を使いこなすには、災害事象を各種要因に結びつけるための知識と経験が必要であるが、ほとんどの企業は災害の要因分析を行う専任者を育てていない。そのため F T A 解析は、上記の専門知識を持たない管理者や安全担当者が行うので、要因を見逃したり、的確な掘り下げができず要因が発散して根源的な事象に到達しない、といったことが起こる。
- ② 各要因の発生確率で判明しているものは少ない。特に「同一条件・環境下」となると「皆無」に等しく、災害発生確率は計算できないかあるいはできても信頼性が低い。
- ③ 日本においては「事故・災害のほとんどはヒューマンエラーで起こる」という前提に立っている

ため、設備上の安全対策の不備と作業標準書や教育・訓練の不備といったヒューマンエラーが同じ重みを持つ要因と結論されやすい。

- ④ 上記①～③より多種多様な要因について、どの対策をとれば確実な再発防止ができるか論理的に判定できず、実施すべき対策の絞込みができない。

これらのことから、根源的な要因の絞込みとこれに基づいた再発防止対策の優先順位を論理的に判定できない場合が多く、F T A が生産現場の労働災害分析に使用されることは少ない。また、実施している企業でも根源的な要因の抽出と有効な再発防止対策に寄与しているとはいえない。

そこで上記の欠点を解消するため、杉浦^{*1)}の提案したリスク = [危険源 (Hazard) の有無の 2 値 × [暴露 (Exposure) の有無の 2 値] の式により、2 値の AND 積論理としてリスクの有無を確定的に捉える「確定的リスクアセスメント」と、国際安全規格におけるリスクの評価方法および安全方策の優先順位を結びつけることで、機械災害におけ

1) T C - 2 主査

〒520-1502 滋賀県高島郡新旭町大字針江 5-343 Tel:0740-25-5686

2) 日本産業ガス協会 常務理事

〒130-0026 東京都墨田区両国 3-21-16 Tel:03-5625-6041

キーワード：リスク、安全確認型、危険検出型、ヒューマンエラー、確定的 FTA (HEFTA)、2 値論理

る根源的な要因と再発防止対策を誰でも簡単に確定することができる「確定的F T A :HEFTA 分析法」を考案したので報告する。

2. 第1ステップ（「確定的リスクアセスメント」の適用）

ISO12100-1:機械類の安全:基本概念（以下「国際安全規格」という）では、リスクとは「危害の発生確率とひどさの組み合わせ」と定義されている。しかし、エネルギーを持った機械による身体的障害又は健康障害である危害は、図1に示すとおり、危険源（Hazard）である機械の稼動領域と人間の作業領域が重なった部分（危険領域）に人が暴露（Expose）された状態（危険状態）においてのみ発生する。

このことを踏まえて杉浦は、リスクアセスメントを「傷害のひどさ（Severity）＊「起こる可能性（Probability）」の組み合わせとして確率的に論じるのではなく、「危険源（Hazard）の有無の2値」×「暴露（Exposure）の有無の2値」とすることで、リスクの有無を2値のAND積論理として確定的に評価することを提案した。

この杉浦の考えに従い、第1ステップでは、トップ事象の要因を、「危険源（Hazard）」と「暴露（Exposure）」に分けることから始める。すなわち災害発生の第1要因を、①危険源・危険状態を作り出す要因の有無、②暴露状態を作り出す要因の有無、に区分する。これにより第1要因は2値で確定的に特定できることになる。

3 第2ステップ（国際安全規格におけるリスクの評価方法および安全対策の優先順位の適用）

日本では「事故・災害のほとんどはヒューマンエラーで起こる」という前提に立っている。このため、F T Aで災害分析を行う場合、ヒューマンエラーを生じさせたもの・状態が災害の主たる要因と判断され、ヒューマンエラー対策を実施することで「危険源・危険状態」及び「暴露状態」を「有」から「無」に出来ると判断するケースが多い。

一方国際安全規格では、機械は故障する、人は間違いを犯す、との前提に立って、リスクを低減させるために採るべき安全対策の順位を、①本質安全対策、②安全防護、③補助安全対策、④使用

上の情報、と定めている。

3.1 《危険源・危険状態》を作り出す要因

3.1.1 本質安全対策

電気・蒸気など動力源となるエネルギーの供給を受けて作動する機械類が危険源となる。これらの危険源は、危険源そのものを排除するか、もしくは保持するエネルギーが人体に危害を与えるほど大きくないように低減する（以下これを「本質安全状態」という）ことで危険源でなくなる。このことから《危険源の有》を作り出した要因の第1は、「本質安全状態」を作り出すための安全対策（以下「本質安全対策」という）の欠如といえる。

3.1.2 停止安全対策

電気・蒸気など動力源となるエネルギーの供給を受けて作動する機械類は、エネルギーの供給を停止して内部に蓄積したエネルギーを放出（開放）した状態（以下これを「停止安全状態」という）では危険源でなくなる。このことから《危険源の有》を作り出した要因の第2は、「停止安全状態」を作り出すための安全防護（以下「停止安全対策」という）の欠如といえる。

停止安全対策には、危険な状態が生じてないか否かを検知して危険な状態が生じた時に情報を出して設備を停止する手段（これを「危険検出型」という）と、安全な状態にあるかどうかを検知して安全な時だけエネルギーを供給して運転を行い、安全な状態が確保できなくなったら直ちにエネルギーを遮断して運転を停止する手段（これを「安全確認型」という）の2種類がある。「危険検出型」の場合、検知手段、情報の伝達手段あるいは停止手段が故障すると設備が停止しないという本質的な欠陥がある。これに対して「安全確認型」は検知手段や情報の伝達手段が故障すると設備が自動的に停止するので常に安全を確保できる。このことから「危険検出型」より「安全確認型」のほうが停止安全対策としてのレベルは高い。

3.1.3 補助安全対策

停止安全対策がなにかの原因で機能しなかった場合に、手動で停止安全状態を作る手段（補助安全対策）として人が緊急時に作動させる非常停止スイッチなどがある。

このことから《危険源の有》を作り出した要因

の一つとして、人が緊急時に作動させる非常停止スイッチなどのような「補助安全対策」の欠如が上げられる。しかし、これらの対策は、人が緊急時に作動させる必要があることから、国際安全規格では安全防護の補助としての位置付けでしかない。また補助安全対策は下記「使用上の情報」と同様に教育・訓練を含めた安全管理体制が良好でないと機能しないので、本質安全対策や停止安全対策に比べ安全確保のレベルは低い。

3.1.4 使用上の情報

《危険源の有》を作り出した要因の一つとして、停止スイッチを手動で操作することでエネルギーの供給を停止させ「停止安全状態」にするなど、作業者に適切な行動をとらせるための標識あるいは作業標準書など「使用上の情報」の欠如が上げられる。しかし、これらは上記補助安全対策と同様に作業者に適切な行動をとらせるための教育・訓練を含めた安全管理体制が良好でないと機能しない。

3.2 《曝露状態》を作り出す要因

3.2.1 本質安全対策

電気・蒸気など動力源となるエネルギーの供給を受けて作動する機械類は、曝露状態を排除するか、あるいはたとえ危険源に接触しても危険源から伝達されるエネルギーが人体に危害を与えほど大きくない状態（「本質安全状態」）では「被害の程度が許容できないほどの《曝露状態》」にはならない。このことから《曝露状態の有》を作り出した要因の第1は、「本質安全状態」を作り出すための安全対策（本質安全対策）の欠如といえる。

3.2.2 隔離安全対策

危険源を完全に囲い、さらに破片、熱、電磁波といったエネルギーの放出を閉じ込めた状態（以下これを「隔離安全状態」という）では曝露状態でなくなる。このことから《曝露状態の有》を作り出す要因の第2は「隔離安全状態」を作り出すための安全防護（以下「隔離安全対策」という）の欠如といえる。

隔離安全対策には、開閉できないカバー等で完全に危険源を密閉化する方法、及び、開閉できるカバーや柵を設けるが、人がカバーや柵に近づくかどうか（曝露状態が生じるか否か）を検知して暴

露状態が生じる前に情報を出して隔離安全状態を作る（カバーや柵を閉止する）「危険検出型」と、隔離状態にあるかどうか（カバーや柵が閉止しているかどうか）を検知して隔離状態にある時だけエネルギーの供給を許可し、隔離状態が確保できない場合はエネルギーの供給（運転）を許可しない「安全確認型」の2種類がある。両者の安全レベルの相違は、3.1.2に述べた通りである。

3.2.3 補助安全対策

隔離安全対策がなにかの原因で機能しなかった場合に、手動で隔離安全状態を作る手段（補助安全対策）として、曝露領域に身体の一部が届かないようにするための安全帯の設置及び人が緊急時に作動させる遮蔽扉・柵などがある。このことから《曝露状態の有》を作り出した要因の一つとして、「補助安全対策」の欠如が上げられる。しかし、これらの対策は、人が装着するあるいは作動させることを前提としているため教育・訓練を含めた安全管理体制が良好でないと機能しない。

3.2.4 使用上の情報

《曝露状態の有》を作り出した要因の一つとして、手動でカバーや扉などを閉止して施錠するなど作業者に適切な行動をとらせるための標識あるいは作業標準書など「使用上の情報」の欠如が上げられる。しかし、これらも作業者に適切な行動をとらせるための教育・訓練を含めた安全管理体制が良好でないと機能しない。

3.3 国際安全規格における安全対策の階層的解析に基づく第2要因以下の確定

国際安全規格のリスクアセスメント規格（ISO14121）に従えば、第2ステップで解析すべき要因は、〔危険源・危険状態〕及び〔暴露状態〕を「有」から「無」にするための安全対策である。これらの安全対策が3.1及び3.2に述べた順番で検討され、実施されており、かつ確実に機能しておれば災害は起こらなかったはずである。これらの安全対策を検討して実施したか否か、および機能したか否かはいずれも2値であり、かつ論理的・確定的に判定することができる。

すなわち、ここでは、危険源・危険状態及び曝露状態について、①本質的な安全対策ができるのにしなかったのか、②本質的な安全対策ができな

い場合で、「安全確認型」安全防護対策を採用することができるのに採用してなかったか、③「危険検出型」安全防護対策を採用することができるのに採用してなかったか、というようにその優先度（安全確保の確実性のレベル）に従い階層的に一つ一つ解析して確定していくことになる。

4. 第3ステップ（根源的要因の特定と再発防止対策の確定）

「上位の安全対策を実施できるのに実施してなかった」、あるいは「実施していたが機能しなかった」という結果に行き着けば、それが根源的な要因であり、解析はここで終了する。そして、優先されるべき再発防止対策はこの要因に対応する安全対策である。すなわちこの手法では要因と優先すべき再発防止対策とが一致する。なお、《危険源の有無》及び《暴露状態の有無》からそれぞれ根源的な要因に対応する再発防止対策が確定されるが、一般的には危険源を無にすることの方がより本質的な対策であるので優先されるべきである。また、危険源及び暴露両方の再発防止対策を採る必要はなく、両者を比較してより優先順位の高い再発防止対策一つを採用すれば良いことが多い。上記確定的 F T A の概念を図 1 に示す。

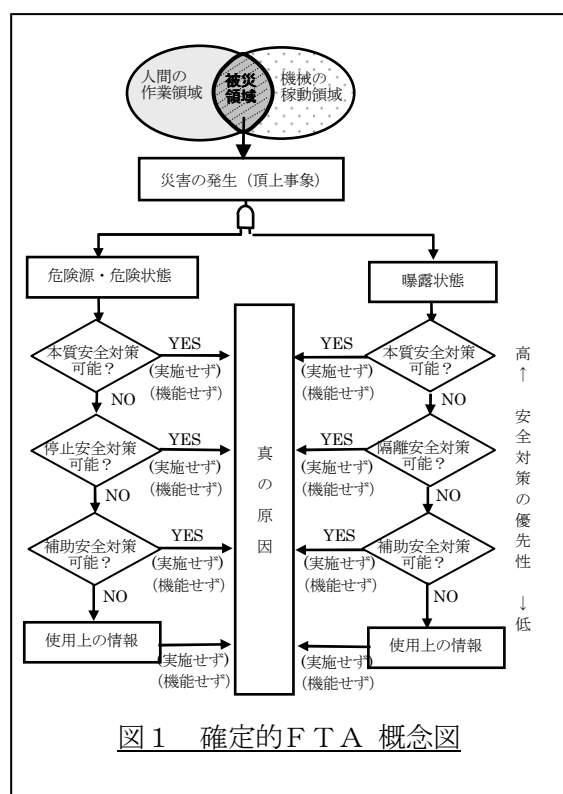


図1 確定的 F T A 概念図

本概念を基に、具体的に解析を行うためのフローチャートを図2に示す。図2の特徴は下記のとおり。

- ①フローチャートの順序および例示の表現に従って事実を記入するだけでよく、特別の FTA に関する専門知識を持たない管理者や安全担当者でも使用できる。
- ②要因抽出における抜けが生じないように、エネルギーで作動する危険源の起こりえる異常状態およびその危険源により起こり得る曝露状態のすべてを網羅してある。

5. 結論

- (1) リスク = [危険源 (Hazard) の有無の2値] × [暴露 (Exposure) の有無の2値] の式により、2値 AND 積論理としてリスクの有無を確定的に捉える確定的リスクアセスメントと国際安全規格におけるリスクの評価方法および安全対策の優先順位を結びつけて、機械災害における根源的な要因と再発防止対策を論理的に確定する「確定的 F T A」を考案した。
- (2) 本 F T A は①「有、無」「実施、非実施」「機能、非機能」の2値により要因を確定する、②確定された要因＝再発防止対策、という構造をもっている。そのため、①災害分析の専門家でなくても実施できる（但し、国際安全規格の概念と主たる規格の概要を理解していることが必要）、②根源的な要因を見逃すことはない、③再発防止対策の優先度判定は国際安全規格に合致しており、客観性・説得力がある、という特徴を持つ。
- (3) 本確定的 F T A のコンセプトは、機械災害だけでなく、職業性疾病、爆発・火災などその他の災害解析にも普遍的に適用可能である。

引用文献

- {1} 杉浦；31 回日科技連信頼性シンポジウム
「ヒューマンファクターを考慮した
確定論的リスクアセスメント法
(AMHEA 分析法) の提案」

記入要綱
 ① _____部に事実を記入する。
 ② < >内はその前に記載した表現の別表現につき、どちらかを選択する。
 ③ ()は _____部分の説明事項につき、事実を記入したら削除する。
 ⑤ フローの点線部は、確定したら実線に変更する。

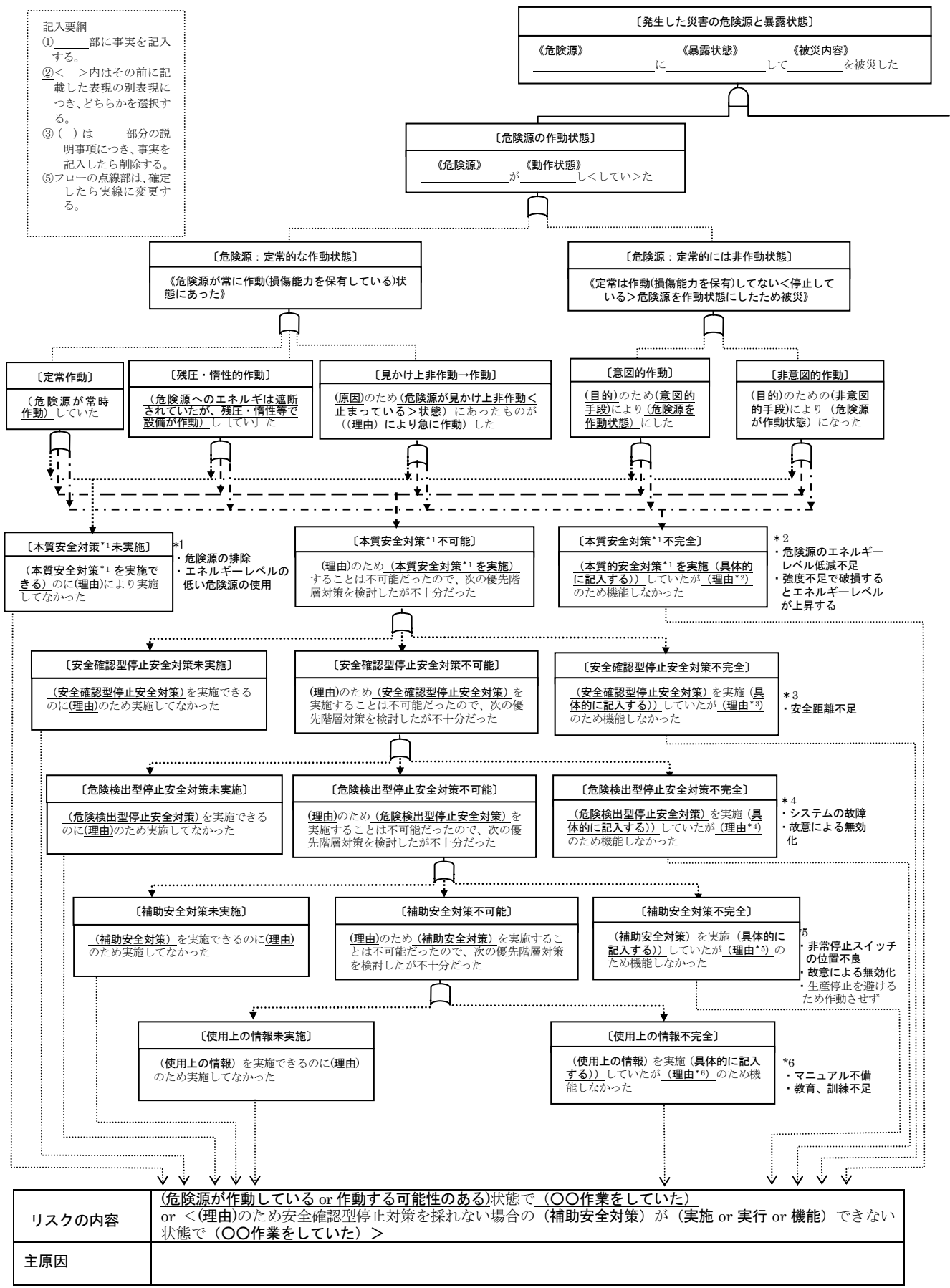


図2 HEFTAフローチャート

