第4章

FTA（故障の木解析）の実施手順

1 FTAの概要と位置づけ
2 FTAの正しい実施手順

（章のねらい）

FTA（Fault Tree Analysis：故障の木解析）は，もともと米空軍のミサイル発射管制システムの予防すべき重大な事象の要因を洗い出すという信頼性評価を行うための手法として開発されました。

機器内部の故障，製造過程における不良品の混入，また外部環境の影響などによる発射失敗の確率を把握することを目的としています。

FTA は，すでに発生している過去の不具合の原因を究明するためのツールではありません。

システムや製品の設計時点で，不具合の発生や，使用時の誤操作を予測して未然防止を図り，市場で問題が発生しないように信頼性や安全性を確保するためのツールです。

この章では，FTA の概要と実施手順，信頼性解析としての FMEA との考え方の違い，特徴，メリット・デメリットについて，いくつかの実施事例を基に解説します。

1．FTAの概要と位置づけ

FTA は日本においても，自動車，家電製品などで広く使われるようになり，市場における重大な事故の未然防止のための有効な手段として位置づけられています。

JISC 5750–4–4 2011：システム信頼性のための解析技法–故障の木解析（FTA）によると FTA は以下の2種類のアプローチ方法があるとしています。

- ●定性的なアプローチとして，起きてはならないシステムや製品の不具合（トップ事象）の要因を洗い出して未然に不具合の発生を防止する。
- ●定量的なアプローチとして，システムや製品の総合的な信頼度又は故障の発生確率を求める。

いずれのアプローチも，設計段階における信頼性解析手法として位置づけられます。

したがって，発生した不具合事象の原因解析の手段としては用いません。

FT（故障の木）図は，トップ事象を起点としてツリー状に展開し，AND/OR などの論理記号を用いて段階的に中間事象から基本事象までを抽出し，解析を行います（**図4–1**）。

1.1　FTAで使用する記号

FTA は，ツリー状に展開する際に，論理記号で結ぶという特徴があります。それはもともと，ミサイル発射失敗の確率を定量的に把握するために AND/OR の論理式を用いたためです。

ただし，定性的な解析においても，中間事象や基本事象の関係性を，AND/OR 条件で分析することにより，システムとしての冗長性の有無や事象の発生条件を解明することが可能となります。

FTA で使用する記号を**表4–1**に示します。

1.2　FT図を論理的に作成する

FTA では，中間事象や基本事象を抽出する際に，無秩序に FT 図を作成するのではなく，一定のルールの基に作成しなければなりません（**図4–2**）。

『ロジカル・シンキング』（東洋経済新報社，

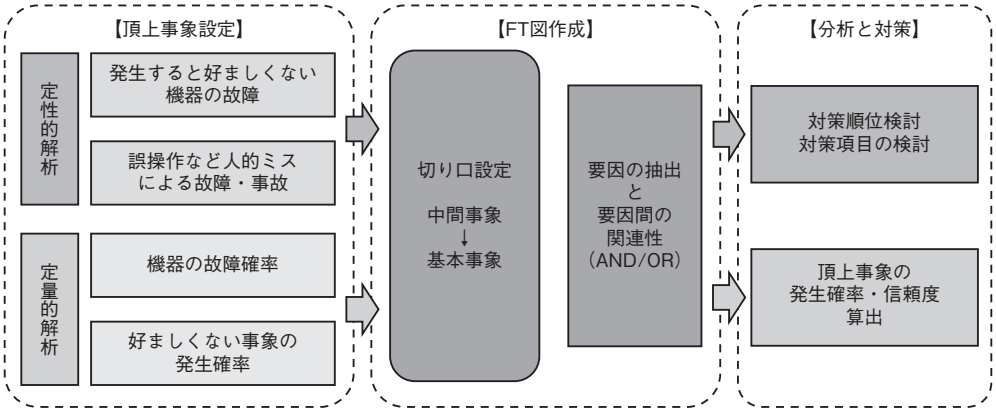

図4–1 FTAの概念図

表4–1　FTAで使用する記号

事象記号	頂上事象 中間事象	頂上事象：解析対象の製品や作業などで発生しては困る事象をFT図の解析目標として明記する。
		中間事象：頂上事象と基本事象との中間の事象を表し，製品など構成を基に表現される事象である。
	基本事象	頂上事象を発生させる原因のうち，分解ができないあるいはそれ以上分解を必要としない事象である。一般的には，対策ができるレベルの事象とする。
論理記号	ORゲート	入力事象のいずれかが発生すると出力事象が発生する。入力事象の数に制限はない。
	ANDゲート	入力事象のすべてが同時に発生した場合に出力事象が発生する。
	移行記号 （入力）（出力）	FT図が大きくなって，別の紙面に書く場合に，三角形の中に分類番号などを書き入れる。別紙面では同じ番号を三角形の中に書き，これを頂上事象としてFT図を作成する。

2001年）の中で，論理的に正しく物事を考えるための基本ツールについて解説されています。

ロジカル・シンキングの基本は，物事を分解して階層（ロジックツリー構造）で捉えることと，漏れなくダブリなく考えることの2つです。

そもそも分析するとは，複雑なものを抜けやダブリがないように順番に何段階にも分けてわかりやすくしていく作業のことです。そうすることで，自分の考えを整理していくことができます。

そのため，トップ事象はできるだけ狭い範囲の事象を設定し，解析の範囲もできるだけ狭く設定します。たとえば，「自動車のエンジンが始動しない確率」ではなく，範囲を絞って，「冬季におけるバッテリーシステムの出力低下によるエンジンが始動しない確率」などとします（トップ事象の純粋化）。

MECEとは，Mutually Exclusive and Collectively Exhaustiveの英語の頭文字を並べたもので，「相互にダブリがなく，全体として漏れがないこと」を指します。

ダブリがなく漏れもない適切な切り口（フレームワーク）の設定とは，たとえば製造業では，4M（人，機械，方法，材料），QCD（品質，コスト，納期）などはよく使われる切り口です。そうすることによって，ダブリや漏れがなくなるだけでなく，解析の根拠が明確になり，第3者による検証も可能となります。

つまり，FT図は誰が見ても納得がいく論理的な階層と切り口を持っていなければなりません。作成根拠が明確でないFT図は，漏れがないかどうかの不安を生じさせ，しかも正しいかどうか検証もできません。

適切な切り口の設定方法は，解析の具体的手順の中で解説します。

1.3　FMEAとの違い

FTAとFMEA（第5章で詳述）はよく使われる信頼性・安全性解析ツールですが，その特徴，使い方の違い，できることとできないことをよく理解

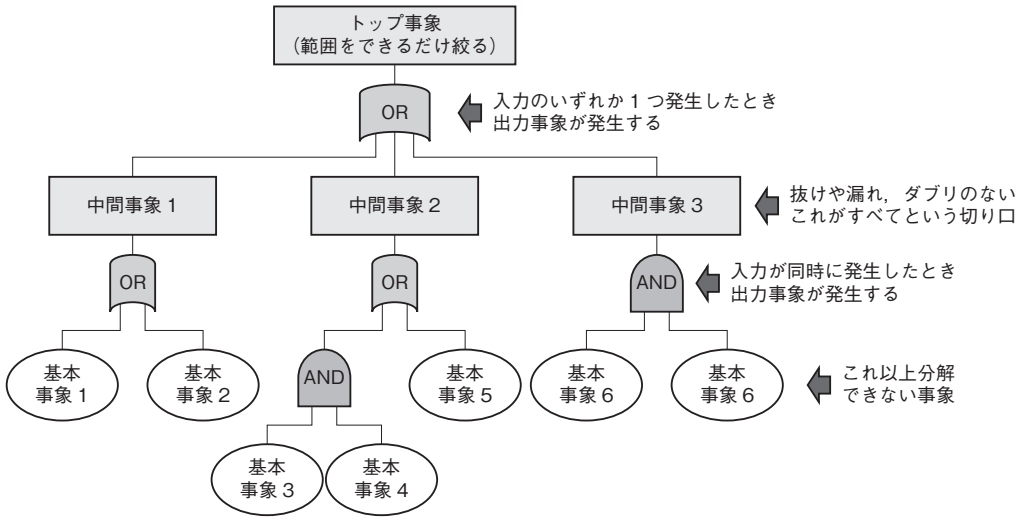

図4–2　FT図の作成方法

し，使い分けていくことが必要です。

(1) トップダウン解析

FMEA は，製品を構成する部品やコンポーネントの故障モードを出発点として上位システムや製品の故障を洗い出すというように，ボトムアップ解析を行います。

FTA は，システムや製品の故障など，起こしてはならないトップ事象を設定して，ピラミッド状に展開し，すべての要因を部品レベルまで探るトップダウン解析を行います。

(2) ヒューマンエラーも対象

また FTA は，トップ事象として，起こりうる誤操作などのヒューマンエラーの要因の解析，設計不良や製造不良の要因解析にも適用が可能ですが，製品の設計 FMEA では，部品の故障モードから導かれる製品の故障のみが対象となります（製造工程の FMEA では，作業ミス：ヒューマンエラーも対象となります）。

(3) 既知の事象の要因を探る

FMEA が「どんな事故が起きるかわからない」という未知の故障の原因を探るのに対して，

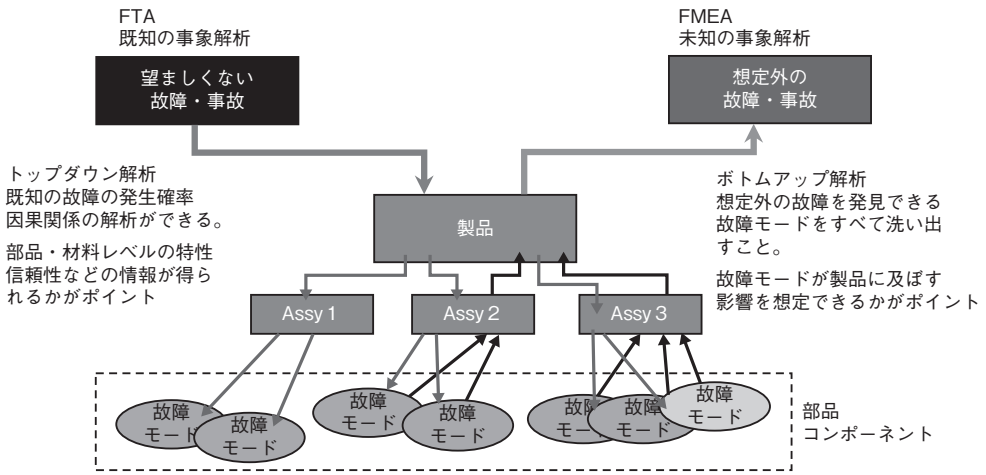

図4–3　FTA と FMEA の違い