SE 17 − 2
(1976. 11. 12)

FTA (Fault Tree Analysis) の応用によるマン・マシン コンピュータシステムの信頼度評価

吉本英明
(日本国有鉄道 鉄道技術研究所)

1. まえがき

Computer 利用の On-line Real Time System を中心とする大規模システムの信頼度評価は、これらシステムの社会的使命、システムの休止がもたらす損失の広範性からみて極めて重要な作業であることはいうまでもない。

しかしながら、従来、システムの信頼性の問題は、どちらかといえばハードウェア中心に取り扱われ、システムのオペレーション，保全等に関与する人間要素やコンピュータのソフトウェアの信頼性を別個の検討対象としてきた傾向が強い。 ところが現実のシステムの運用実績の多くは、これら人間要素やソフトウェアが原因でシステムダウンとなる場合が極めて大きな割合を占めていることを物語っている。 しかも、障害の個々の内容を調べてみると、システムの設計思想にさかのぼってハードウェアを含めて相互に複雑にからみあっていることが少くない。 したがって、オペレータの誤操作やソフトウェアのトラブルをハードウェアと等価に見立てたシステムコンポネントとして取扱うことは適当ではない。 また、システム故障の多くはシステムの外的条件が乱れた異常時に発生することもしばしば経験されるところである。 つまり現実に則したシステムの改善の立場からは、外乱を何らかの形でシステム評価モデルに導入することが望まれる。

このような観点から、大規模システムの運用状態における実際的な評価モデル、すなわちハードウェア、ソフトウエア、人間要素およびシステムに加わる外乱の相互関連を明らかにするためのモデル化手法のひとつの試みとして FTA (Fault Tree Analysis) の応用を提案する。

2. FTA の概要と特長

FTA は 1962 年に Bell 研究所の Watson が対空システムの安全性解析のためのモデルとして示したのが最初といわれている。 FTA はシステムの致命的(重大)な故障の要因をシステム開発の早期段階で予測し、安全性・信頼性の向上のための効果的・経済的な対策を組織的に見出すことを目的としている。 FTA はまた LDA (Logical Diagram Analysis) の名でも呼ばれる如く、故障の発生メカニズムをブール代数的論理関係に展開して表現することに大きな特長がある。

故障発生の様態を、システム構成要素の故障モードに着目して組織的に解析する手法としては FMECA (Failure Mode, Effect and Criticality Analysis) もよく知られているが、FTA とは対照的な点が多い。 両手法の違いを対比しつつ FTA の特長を挙げれば次のとおりである。

(1) FTA はまずはじめにシステムの「望ましくない状態 (Undesired Fault)」を規定する。これを Top Event とも云う。 そして「Top Event

はどういう状況のもとに起こるか」をサブシステム，コンポネントのレベルに順次もとめていく、トップダウンのアプローチである。　これに対してFMECAは、まず部品の故障モードに着目し、それが上位のサブシステム，システムにどういう影響をもたらすかを順次吟味するボトムアップのアプローチである。

（2）　FMECAは一般にハードウェアの故障のみを対象とするのに対し，FTAは人間の誤操作や外部条件などを関連づけて表現できる。

（3）　FMECAは実際上単一故障しか扱えないのに対し，FTAは複数の要因の競合による故障を表現できる。

（4）　FMECAは解析結果がテーブル形式で示されるのに対し、FTAは論理記号を用いたトリー構造に図示されるので、非専門家にも視覚に訴えて直観的に理解しやすい。

FTAは各要因の因果関係をブール代数論理記号を用いて表わすが、記号の標記法はまだ一般的に標準化されていない。　本文中では図1のように表わすことにする。　このほかに、事象間の順序関係や遅延を表わす記号や、多数決論理を表わす記号を用いることもある。

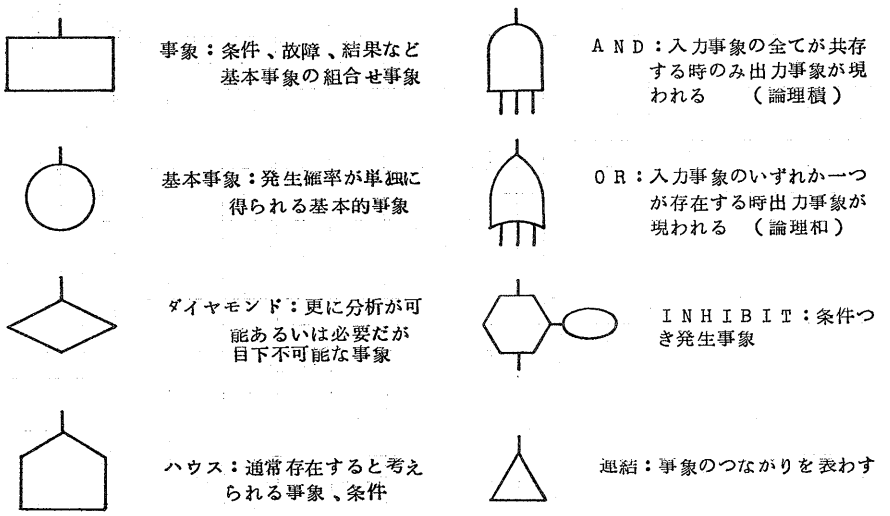
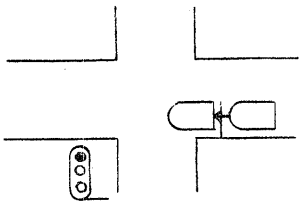
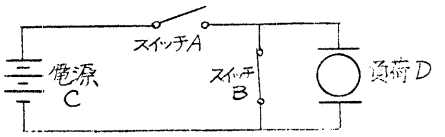


図1　FTAに用いる主な論理記号

FTAの簡単な例を図2および図3に示す．　図2は交叉点において停止信号を（結果的に）無視して信号冒進することをTop Eventとしたfta の例である．　原因を大別すると、自動車のブレーキ機構の欠陥，ドライバのミスおよび地上の信号機機構の異常の3つが考えられる。　ブレーキ故障については更に分析を進めることが可能であるが省略したのでダイヤモンドで示してある。





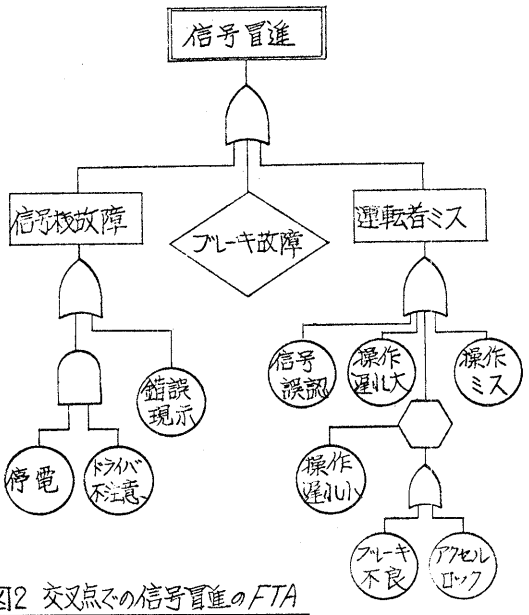


図2 交叉点での信号冒進のFTA

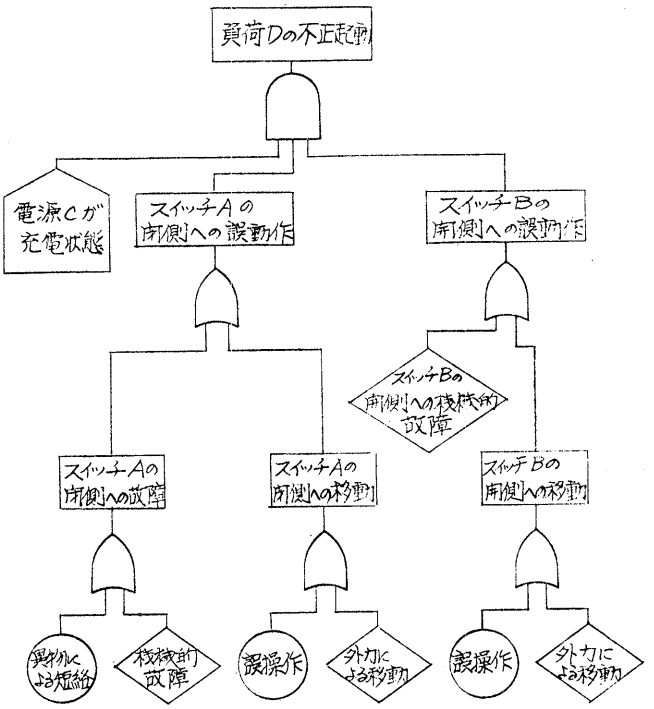


図3 電動機の不正起動のFTA

図3で、回路のスイッチAは負荷Dに電源を投入するスイッチで、スイッチBは負荷から電源を解放するための短絡スイッチである。負荷（モータ）が停止の状態であるべき時に不正に起動されることをTop EventとしたFault Treeを示している。電源Cは通常は充電状態にあるものとしてハウスで示している。基本事象としては、操作員の誤りや外力、機械的故障などが考慮されている。また、ここでは考慮されていないが、電源がOFFの状態のとき回路への迷流等による不正起動も考えられよう。

3. マン・マシンコンピュータシステムの信頼度評価への応用例

新幹線が岡山まで延長された昭和47年に列車指令業務の省力化を目的としたコムトラック（COMTRAC）が導入された。このシステムは；

（1） 輸送需要の変動に即応した運転計画の作成と各所への伝達
（2） ダイヤ乱れの検出とそれに対応したダイヤ変更とその伝達
（3） 各駅の進路制御

を主要な機能としてもつ典型的な大規模man-machine Computer Systemである。図4にCOMTRACシステムの構成を示す。

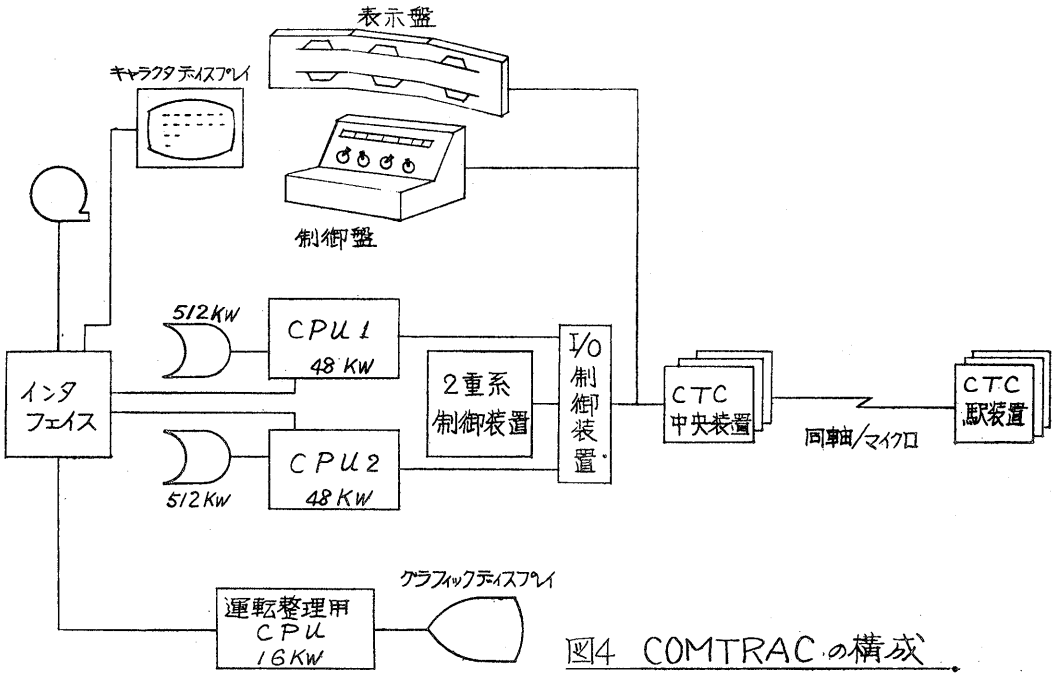


図4 COMTRACの構成

CPU1およびCPU2は、各駅の進路制御および小規模なダイヤ乱れに対する処理を行なう〝進路制御サブシステム〟で、リアルタイム性および出力情報の信頼性が特に重視されるので2重系構成とし、2つのCPUは同じ処理を行ない出力は2重系制御装置で一致検出を行なっている。指令員とのマンマシンインタフェイスにはキャラクタディスプレイを、また各駅との情報伝送にはCTCを用いている。運転整理用CPUは、列車運行状況の監視、ダイヤ修正案の出力による指令員のバックアップおよび運転実績、記録統計などを行なう〝運転整理サブシステム〟で、指令員とのインタフェイスにはグラフィックディスプレイを用いている。

〝進路制御サブシステム〟の運用開始後2年間のシステム障害の状況は、図5のとおりである。ハードウェア以外の障害要因が過半数を占め、システムの信頼性向上のためにはソフトウェアや人間の要因に注目すべきことがわかる。

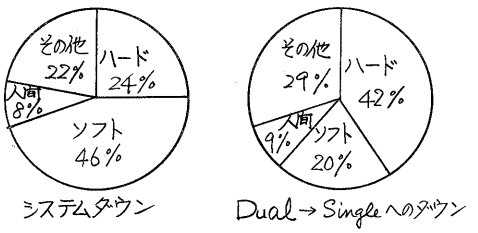


図5. COMTRAC進路制御系の障害要因

システムの障害データから全障害の80%は上記の2つのモードとは別の「列車追跡中断」であることが分った。列車追跡とはコンピュータ内に記憶されている列車ダイヤと、時々刻々CTCを介して伝送入力される各駅の列車検知情報を照合して全線の列車の順序関係を把握する技能である。

列車追跡中断の障害の多くは指令員の絡んだものであった。そこで、これらの障害の発生様態をモデル化し、改善の方策とその効果を明確にする目的でFTAを応用することにした。システム設計にたずさわったメンバーを中心にしてシステムの構造面からの分析と障害事例の分析を行ない、図6のようなTreeが得られた。

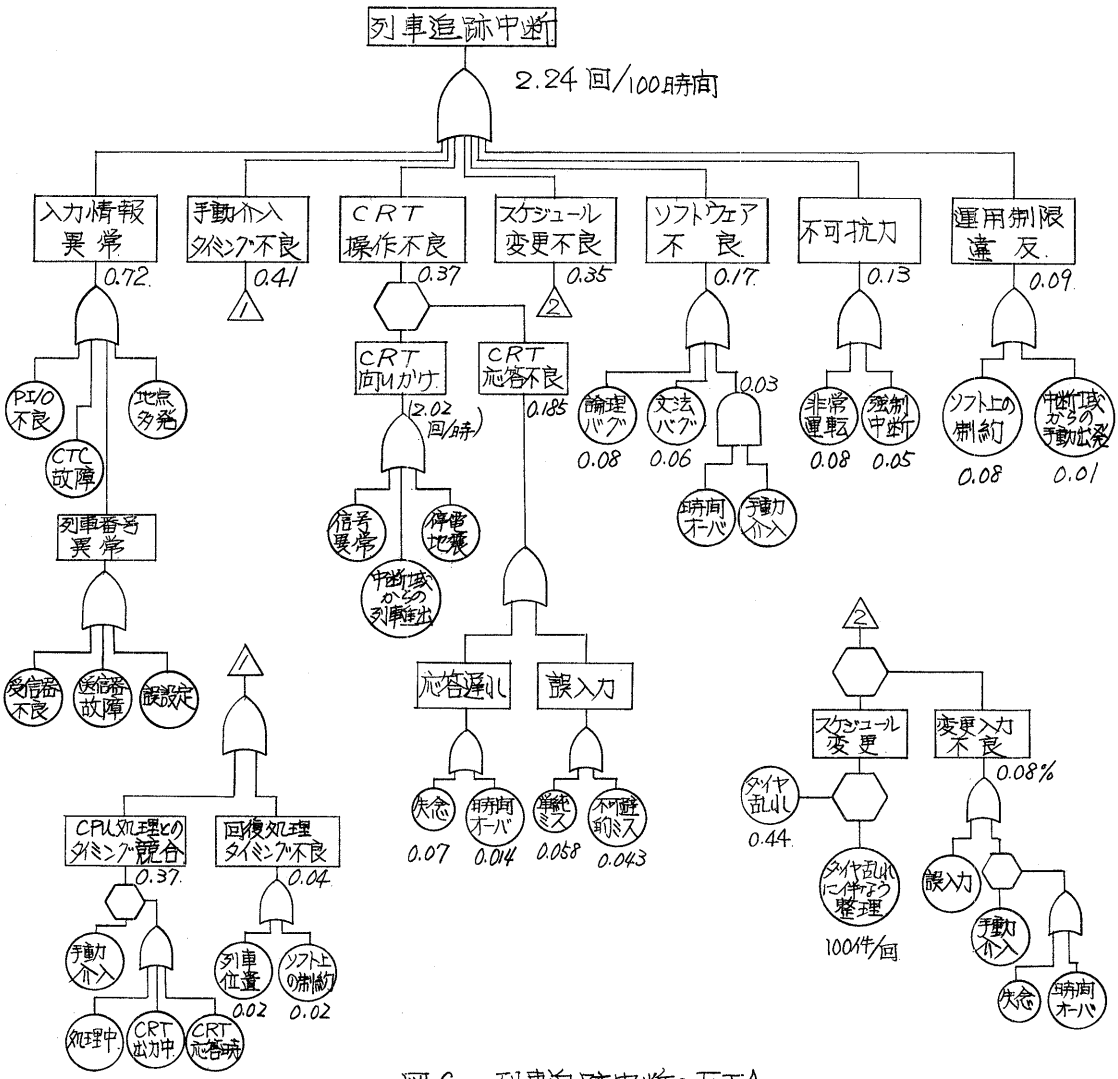


図6. 列車追跡中断のFTA

この解析を通じて判明した主な事項は次のとおりである。

(1) 入力情報異常はハードウェアの要因による中断の大半を占めるが、全体の32%にすぎない。

(2) 手動介入(コンピュータによる制御が渋滞したとき指令員が制御盤から手動で進路を制御する)が、計算機の速度、ソフト上の制約から種々の形で中断に結びついている。

（3）キャラクタディスプレイによる応答でのトラブルが全障害の32%を占める。
（4）ソフトウェア関係は、「バグ」として顕在化するもの以外にシステムオペレーションに種々の制約を課しており、改善を要する。

上記のシステムは、博多開業に伴ない全体を才2期システムに置き換えることになり、FTAによる解析結果も才2期システムの設計にフィードバックされた。そして才2期システムにおける列車追跡中断のFTAによる予測を実施した。結果は図7に示すとおりである。

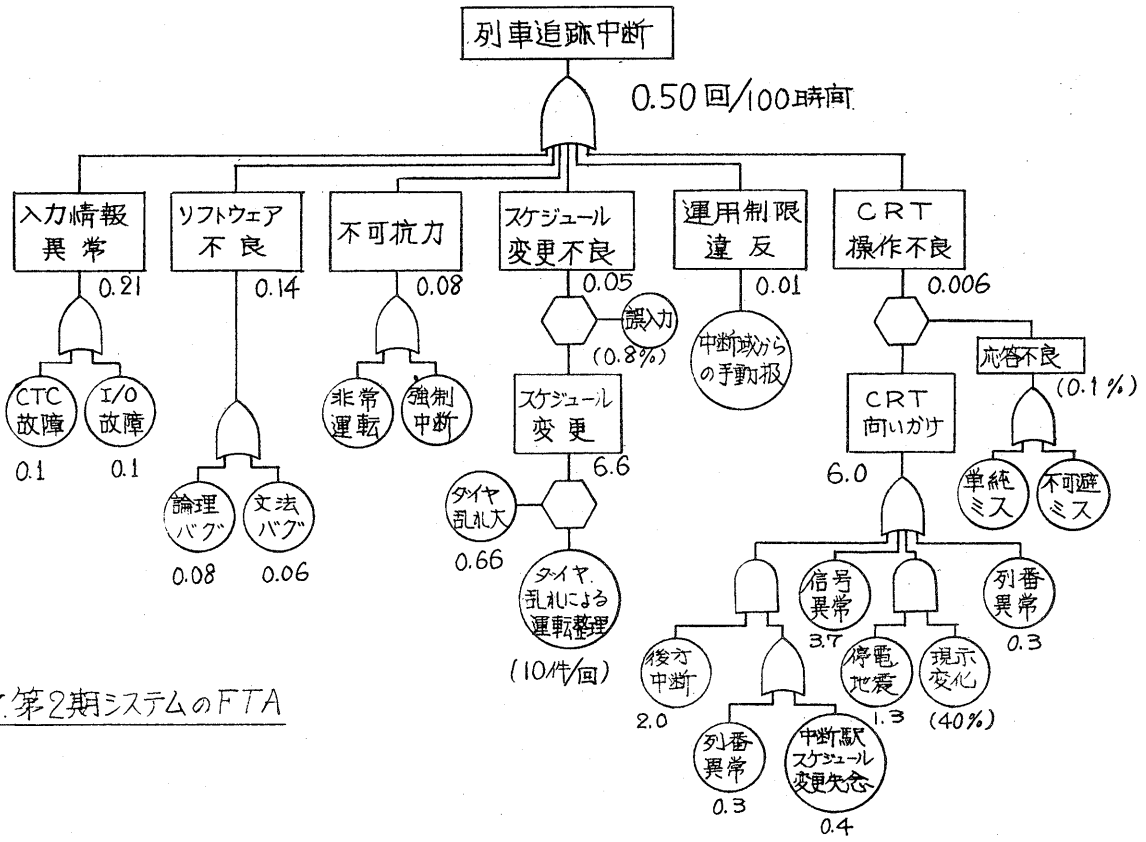


図7. 第2期システムのFTA

才2期システムはシステムの基本的な設計思想に大巾な変更はなかったが、才1期システムの問題点を極力改善したほか、コンピュータの能力アップがなされた結果、特に手動介入および CRT 応答の問題がほぼ解消した。改善の効果を才1期システムと対比して示したのが図8である。制御対象範囲が約50%拡大したが中断発生率が約1/4になったことがうかがわれる。なお博多開業後の実績は、上記の予測をほぼ裏づけるものであった。

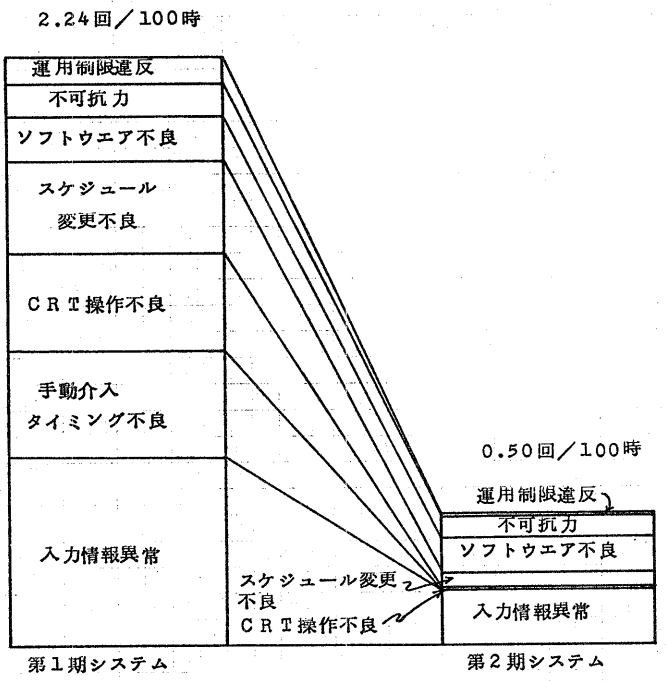


図８　システム改善による障害予測値の比較

4. ＦＴＡの問題点と今後の課題

ＦＴＡは手法が単純明解で特にその表記法は万人に理解しやすい特長がある。しかしその反面、最終的なトリーを得るまでの過程および数量化の局面において隠れた困難がある。とりわけＦＴＡは発見的なアプローチであることから、要因をもれなく完全に網羅することは仲々むづかしい。

筆者のわづかな経験をも含めてＦＴＡの問題点と今後の課題を要約すれば以下のとおりである。

（１）Top Eventの定義があいまいになりやすい。------ＦＴＡはトップダウンの解析であるので出発点にあたるTop Eventは厳密に定義しておく必要がある。その際システムの範囲（ハードウェア，人間，オペレーションモードの範囲等）も明確にしておくことが大切である。

（２）要因をもれなく抽出するのが難しい。-------特に安全性解析においてクリティカルな潜在要因を見落すことは致命的である。そのためにはシステムの構造，異常時対策や外乱に対するシステムの機能限界に精通した設計技術者が解析に参加することが不可欠である。また、数名によるディスカッション形式で解析を進め、見落しや感ちがいを防ぐことも得策である。

（３）数量化のためのデータが入手困難である。------トリーが得られ、基本事象の発生確率に関するデータが得られれば、Top Eventの発生確率は明解に得られる。しかしながら基本事象の多くは一般の障害報告等の顕在化したデータからは直接得られない場合が多い。従ってトリーの作成過程においても基本事象をどのレベルまで掘り下げるかを利用可能なデータが存在するか否かをも考慮

しつゝ吟味する必要がある。　また日常そうした基礎データを収集する努力も必要である。

（4）外乱の定量的モデル化が必要である。------一般にシステムの障害は何らかの外乱が加わった時におこる。　大規模システムにおいては外乱の様態もまた多種多様である。　したがって、より効果的、積極的な改善対策に結びつけるには、これら種々の外乱を定量的なモデルとしてトリーに取り込んでいく必要がある。