信頼性評価技法の情報システムへの適用

2K−4

石塚　隆男[1]，　長沢　伸也[1]，　菊地　玲[2]

[1] 亜細亜大学　[2] 情報処理振興事業協会

1．緒　言

今日，システム設計を成功させるための手法としてＣＡＳＥを始めとしてさまざまな方法論が展開されている。これらの手法の大半はシステムの構造化分析・設計を主眼としており，専ら，システムの論理モデル化を支援するものである。開発段階におけるテストもシステムが要求どおりに動くかどうかに主として関心が払われている。また，信頼性設計ではシステムのセキュリティや障害時の回復についての一般論が中心であり，対象としているシステムの信頼性を網羅的に評価し，設計に反映することは体系的には行われていないのが実情である。

ソフトウェアの信頼性についてはこれまで信頼度成長モデル等，理論的かつ統計的なアプローチがなされてきたが，これらは現象を説明するための手法であり，現実のシステム設計に直接，役立つものではない。

このように運用段階におけるシステム障害を回避するために情報システムの設計段階から信頼性を評価し，不適切な部分があれば設計を見直す手法はまだ，確立されていない。こうした現状を踏まえて，今回，われわれは信頼性評価技法として知られるＦＭＥＡ（Failure Mode and Effects Analysis）並びにＦＴＡ（Fault Tree Analysis）を情報システムの設計に適用することにより知見が得られたので報告する。

2．従来の方法

情報システムは一般にハードウェア，ソフトウェア，並びにヒューマンによって構成されている。従来の信頼性評価技法はハードウェア中心のシステムが対象であり，ソフトウェアや人間が介在するシステムについて総合的な観点から信頼性を評価する手法はまだ確立されていない。

このうち，ＦＭＥＡとＦＴＡは定性的な扱いが可能であり，既に稼働しているシステムはもとよりこれから開発するシステムのように障害データの蓄積がないものにも適用できる。ＦＴＡは結果→原因へのトップダウン型手法であるが，ＦＭＥＡは各機能・プロセスの故障が単独で独立に起きた場合の影響度の解析を行うものであり，原因→結果のボトムアップ型手法とみることができる。

ＦＭＥＡをソフトウェアに適用する場合にはそのソフトウェアの機能ブロック図に相当する資料を入手もしくは作成する必要がある。この観点からシステムの構造化分析手法のひとつであるデータフロー図（ＤＦＤ）を利用することが考えられる。しかしながら，対象が情報システムである以上，狭義のソフトウェアにとどまらず開発・運用に関わる人間，組織まで含めたＦＭＥＡを実施する必要があろう。この点については後述する。

An Application of Reliability Evaluation Technique to Information Systems

Takao Ishizuka [1], Shin-ya Nagasawa [1], Akira Kikuchi [2]

[1] ASIA University　[2] Information-Technology Promotion Agency, Japan

また，ヒューマンファクターの定量的な扱いが困難なため，ＦＴＡを情報システムに適用し，トップ事象の確率的評価を行うことは困難であるが，ＦＭＥＡとの双対性を活かして原因・結果を網羅的に調査し，的確なＦＴＡが作成されなければならない。

3．オブジェクト指向的ＦＭＥＡ

情報システムにＦＭＥＡを適用し，網羅的に故障原因とその影響を解析する方法を提案する。既に述べたようにＤＦＤをもとにしてＦＭＥＡを作成することが考えられる。通常，ＤＦＤはデータの流れを矢印で，プロセスを○（バブル）で，データ蓄積を＝で，外部実体を□で表す。このうち，データの流れ以外をすべてオブジェクトとしてとらえることにする。これによりファイルやデータベースとともにシステムの運用に関わる人間（情報源やユーザーを指す）を取り込むことができる。また，情報システムを構成する各コンポネントの故障モードを網羅的に把握するためにシステムの構成と挙動に区分して考えることにする。

図１にこれらの概念図を示す。

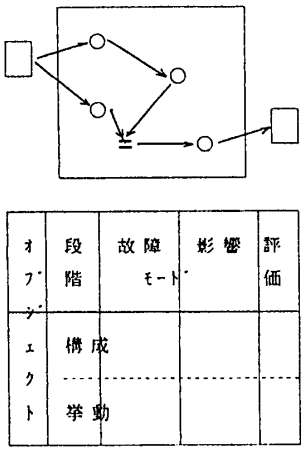

図１．ＤＦＤとオブジェクトＦＭＥＡ

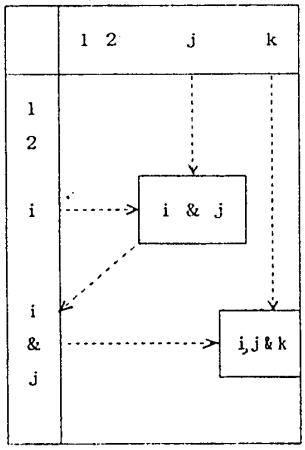

図２．ＡＮＤ故障の創出チャート

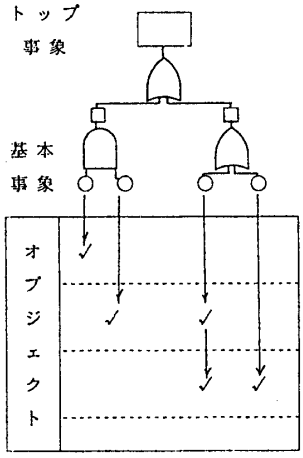

図３．ＦＴＡとオブジェクト

近年，大事故につながるような障害はコンポネントのいくつかに基本事象となる原因が起き，２重，３重のフェイル・セーフ構造になっているにも関わらず，たまたまそれらが働かなかったことに因るものが少なくなく，設計者の盲点をついたものといえる。こうした事故を未然に防ぐためには故障の組み合せによる二次的な故障ないしは影響を設計時点で創出し，ＦＴＡに反映させることが必要である。図２はこれを網羅的に調査するためのチャートであり，図３は各オブジェクトとＦＴＡの基本事象との対応表を示している。図２の関係行列からＩＳＭ法を用い，ＦＴＡのTree構造を作成することも可能である。

4．結　　論

情報システムに信頼性評価技法として知られるＦＭＥＡ並びにＦＴＡを適用するための検討を行った。これらのチャートがいわゆるＣＡＳＥの１ツールとして組み込まれ，システム運用後も障害モニターとして機能することが臨まれる。

本研究は「ソフトウェアの信頼性・安全性総合評価技術の研究開発」（平成２年度ＩＰＡ委託研究）の一環として行ったものである。