ソフトウェア安全性分析へのアプローチ

5N－10

柳生 理子, 中島 毅, 田村 直樹, 萩原 正敏
三菱電機 (株) 情報電子研究所

1　はじめに

近年、ソフトウェア制御によるシステムが社会の重要な部分に使われ、そのシステムの故障がもたらす災害が大きな社会問題となるケースが増えてきている。それに伴い、安全性と言う視点からソフトウェアの品質を保証することが必要になってきているが、ソフトウェアの安全性に関しては、計測と評価を行なう方法が確立していないのが現状である [1]。

本論文では、ソフトウェアの安全性に関わる問題を明らかにし、その解決への指針を示す。以下、ソフトウェアの安全性分析の現状と問題について述べ、これらの問題を解決する為の安全性の技法を提案する。

2　ソフトウェア安全性分析の現状と問題

安全性分析とは、システムが何をしてはいけないかを分析することであり、何をすべきかを決める機能分析と異なる視点を必要とする。従来、安全性分析は、機能分析が終った時点で、関係者が集まりその機能仕様をレビューする方法が主流である [2]。
この方法は、以下の問題点を持つ。

(1) 機能分析と同じ視点である為、設計で想定からはずした状態に、実際には入ってしまうことによる災害や、複数の要因が複雑に絡みあって発生する災害などを見落とす可能性が高い。

(2) 系統だった方法ではなく、ランダムに思い付く事を並べる為、レビューア個人の経験と勘を要する。

3　安全性分析を取り込んだプロセス

従来の方法の問題点 (1) を解決するためには、レビューに至る前の段階で、機能分析と並行して機能分析とは全く異なる視点から安全性に関する分析を行なう必要があると考える。

図 1 は、安全性分析を組み込んだ分析プロセスである。図 1において、安全性要求をシステム要求と別個に仕様にまとめ、相互参照し矛盾を探し、その中から災害となる『問題』を洗い出す。『問題』に対し『対策』を立て、機能仕様に組み込み、再び安全性をレビューする。今回、図 1の丸で囲った安全性分析の部分を、技法の対象とした。

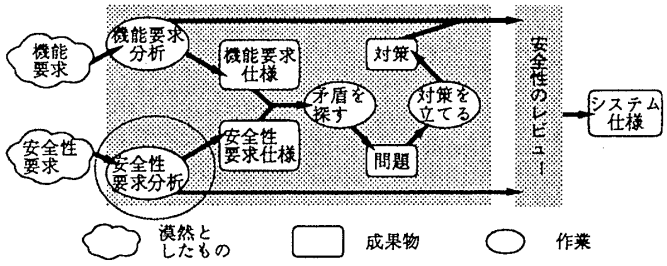

図 1: 安全性分析を組み込んだプロセス

4　安全性分析技法の提案

安全性分析は、一般にシステムのドメインに依存した知識を必要とするので汎用化し難いと言われている [1]。しかし 2 の (2) の問題により、分析をある程度系統だった手順で行なわない限り、いつまでも安全性の面での品質がレビューア個人の能力に依存することになる。

我々は、安全性分析の手順化を行ないつつドメインの知識の蓄積をめざす技法を提案する。本技法の基本的なアイデアは、対象ソフトウェアを取り巻くオブジェクト（システム及びシステムを取り巻く環境を構成するもの）に注目し、オブジェクトから災害を連想的に洗い出すことである。技法は次の 4 つのステップから成る。

(1) オブジェクトの洗い出し
(2) 災害の定義
(3) 災害の要因の洗い出し
(4) 災害発生の過程の定義

以下、各ステップを簡単な例を用いて説明する。

4.1　オブジェクトの洗い出し

このステップではシステムに関係するオブジェクトを洗い出す。この作業では、図 2に示す『外部オブジェクトの洗い出し表』を用いる。図 2において、外部オブジェクトの大分類をシステム構成機器、システムサービスの

An Approach to Safety Analysis for Software
Riko Yagiu, Tsuyoshi Nakajima, Naoki Tamura, Masatoshi Hagiwara
Mitsubishi Electric Corp.

受益者、オペレータ、システムの運用と無関係な外部環境の4つに固定する。小分類は、4つの大分類をドメイ

システム名： 航空機システム No.

オブジェクト分類		具体的オブジェクト
大分類	小分類	
システム構成機器	1 飛行に直接関与する	機体（及びその部品）、滑走路、…
	2 通信に関係する	
	3	
	4	

図 2: 外部オブジェクトの洗いだし表

ンの知識を基に、詳細化したものであり（例えば『システム構成機器』に対する『飛行に直接関わるもの』）、システムのドメイン毎に異なる。オブジェクト名の欄にはさらに詳細な『機体』などを書き込む。

4.2 災害の定義

このステップでは図3を用いて、『機能を実現する手段がもたらす災害』を洗い出す。4.1で洗い出した具体的オブジェクトを置き、表の抽象的な災害の分類をオブジェクト毎に、具体的災害へと詳細化する。抽象的な災害の分類には、身体の損傷と経済的な損傷に対して、それぞれ直接、間接の二つがある。航空機の例では、乗客

外部オブジェクト：乗客 No. 1

抽象的な災害			具体的災害
大分類		小分類	
身体の損傷	1.1	直接的損傷（怪我）	墜落による死傷、落下物による死傷、…
	1.2	直接的損傷（病気）	
	2.1	間接的損傷（怪我）	犯罪に巻き込まれて怪我をする、…
	2.2	間接的損傷（病気）	空調により風邪をひく、 …
経済的損失	1	直接的損失	気圧で物が壊れる、…
	2	間接的損失	予定時間に間に合わない、…

図 3: 機能がオブジェクトに与える災害の洗い出し表

に対する『直接的身体の損傷（怪我）』を『墜落による死傷』などへと詳細化する。この時、特に重要な災害と関わるシステム構成機器オブジェクトに対し、状態遷移図 [3] を作成する。

4.3 災害の要因の洗い出し

4.2で洗い出された各々の災害の要因を、図4を用いて洗い出す。図4で左上の『現象名』に、要因を洗い出す現象を書き、人為的ミス、H/W 的故障、環境条件、それらの復号条件、の4つの分類から連想して、その現象を引き起こす『具体的要因』を記述する。『具体的要因の洗い出し』は、4.2で洗い出された災害からスター

現象名： 航空機が墜落する No. 1

要因		関連事項
分類	具体的要因	
人為的要因	操縦ミス	
	整備ミス	
	誘導ミス	
	操縦側の判断ミス	
	エンジンの故障	油圧系統、…
	機体の損傷	

図 4: 災害の要因の洗い出し表

トし、『洗い出された要因』のさらに詳細な要因を再帰的に洗い出す。関連事項欄には、現象に関連の深いものを記入し、具体的要因を洗い出す時に参照する。

4.4 災害発生の過程の定義

4.2で定義された災害を根に置き、4.3で洗い出された災害の要因を基にして障害分析木を作成する。障害分析木は、災害と要因との間の論理的関係を表す図である。以下図5に、航空機における簡単な例を記す。

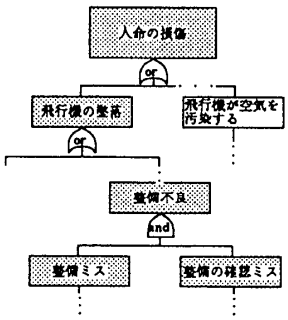

図 5: 災害分析木の例

さらに災害が起こるか否かの確認は、状態遷移図を基に、シナリオ（障害木の根から一つの先端に至る事象系列）[3] を追うことによって行なう。

5 おわりに

本論文では、安全性分析への一アプローチを示した。今後、さらに技法を洗練させ、技法を支援するツールを開発してゆく予定である。

参考文献

[1] N. Leveson, "Software Safety: Why,What,and How," ACM Computing Surveys, Vol.18, No.2, pp.125-163, Sep.1986

[2] NASA-JSC-30309 Instruction for Preparation of Hazard Analysis for the Space Station

[3] J. ランボー, M. ブラハ, W. プレメラニ, F. エディ, W. ローレンセン＝著, 羽生田栄一＝監訳:" オブジェクト指向方法論 OMT − モデル化と設計 "Prentice Hall