2004－SE－145　(15)
2004／8／20

組込みソフトウェア非正常系の概念モデル

新屋敷泰史¶　三瀬敏朗†　江浦洋平††　畑中久典‡
橋本正明‡　鵜林尚靖‡　片峯恵一‡　中谷多哉子‡‡

概要

近年、商品組込み系ソフトウェア（以下、組込みソフトと呼ぶ）の大規模化に伴った開発手法の整備が必要とされている。組込みソフトの要求分析工程での課題は、非正常系仕様の設定に関する方法論が不十分な事である。そのため我々は、組込みソフト分野における非正常系仕様の設定技術について研究している。我々はこれまでの研究で、非正常系仕様の記述における考慮すべき事項の分析を行った。分析を通じて、知識ベース化と言語記述による支援が可能であるとの仮説を立てた。更にこの仮説に基づき、非正常系仕様の知識ベース化を目的として非正常系現象のモデル化を行った。今後は、このモデルの有用性の確認、記述性の充実、モデル活用方法の 3 点について検討する。

A Conceptual Model of Exceptions in Embedded Software.

Yasufumi Shinyashiki¶, Toshiro Mise†, Youhei Eura††,
Hisanori Hatanaka‡, Masaaki Hashimoto‡, Naoyasu Ubayashi‡,
Keiichi Katamine‡, Takako Nakatani‡‡

Abstract

Recently, embedded software needs the improvement of development methodology because of increasing scale. An important problem in requirement analysis of embedded software is lack of methodology that handles exceptions. Therefore, we studied about exception handling methodology in embedded software. We analyzed what should be considered about exceptions in embedded software. We also made a hypothesis that we can help handling exceptions with knowledge base and specification description language. Then, we developed a model of exceptions for developing knowledge base of exception specifications. We will discuss the effect, constructability and applicability of this model in the future.

¶.松下電工株式会社/九州工業大学
Matsushita Electric Works, Co., Ltd. / Kyusyu Institute of Technology
†.松下電工システムソリューション株式会社/九州工業大学
Matsushita Electric Works System Solution, Co., Ltd. / Kyusyu Institute of Technology
††.松下電工株式会社
Matsushita Electric Works, Co., Ltd.
‡.九州工業大学
Kyusyu Institute of Technology
‡‡.九州工業大学/有限会社エス・ラグーン
Kyusyu Institute of Technology / S-Lagoon Co., Ltd.

１．はじめに

近年、組込み系ソフトウェア（以下、組込みソフトと呼ぶ）の大規模化、複雑化が進む一方で、開発期間の短縮に対する要求が強くなっている。例えば経済産業省が実施した調査[1]によれば、仕様設定や設計段階における問題が重要である事を裏付ける統計結果として、以下のようなものが挙げられている。

･組み込みソフト関係者の約 70%が、課題はソフトウェアの品質向上にあると認識している

･外注発注時の課題のトップに、要求仕様や設計仕様の伝達の困難さが挙げられている

･開発中発生した前工程への手戻りの原因のうち、要求仕様や仕様書の不備が約半数を占める

このため、組込みソフトに対しても効率的な開発手法の整備が急務とされ、様々な手法が提案されている。しかし仕様分析段階においては、組込みソフト固有の特性から、それらの手法が十分な効果を発揮できていないと思われるのが現状である。

組込みソフトには、長期安定動作、ユーザーの監視下にない状況での動作、リアルタイム性、消費電力・発熱への配慮、多少の異常がある状態でも動作を保証するといったユーザーからのニーズと、ハードリソースの制限、開発中のハードリソース変更に対する対応といったメーカーからのニーズがあるという特徴がある。これらのニーズに対応するためには、開発者にハードウェアに対する知識とソフトウェアが利用される環境におけるシステムの障害要因となりうる事象や状態（以下、システムの障害要因となりうる事象や障害が発生している状態を総称して非正常系と呼ぶ）に対する知識が必要となる。実際、組込みソフトに関する市場で散見されるトラブルは、その多くが非正常系への対応が不十分であった事に由来するものである。この事からも、非正常系に対応するための仕様（以下、非正常系仕様）を正しく効率的に設定できれば、組込みソフト開発に対する大きな改善効果が期待できる。

このような背景に対して、現在のソフトウェア工学分野の関心は、設計以降の段階や、プロダクトライン等を初めとするメタ的なレベルでの開発に集まっている。それらの研究においては、非正常系仕様の適切な抽出は、開発者が独自に達成している事を前提としている。そのため、もし非正常系の仕様記述について適切な方法論を提示する事ができれば、これら周辺の段階に着目した研究と合わせ、組込みソフトの開発に大いなる効果が期待できる。

以上の背景から我々は、非正常系仕様の形式的な記述方法を規定するための概念モデルを提供する事によって、組込みソフト開発の支援を行う方法を研究している。以下本稿では、第 2 章にて非正常系の事例分析を述べ、第 3 章で分析結果をもとにした非正常系の概念モデルについて述べる。第 4 章では提示した非正常系の概念モデルについて、その妥当性を考察する。そして第 5 章では、本研究における今後の課題について述べる。

２．非正常系仕様の事例分析

我々は最初に、組込みソフトにおける非正常系仕様の記述のもととなるモデル構築を目的として、非正常系仕様の設定において考慮すべき事項について過去事例の分析を行った。本章では、分析の結果得られた事項を示す。ここで各事項を通じた具体例として、以下のような単純な架空商品を想定する。この商品は屋外に設置される照明器具であり、センサ部に入る一定以上の光量である場合に+5V の電圧を出力する昼光センサと、辺りを照らす

照明器具及びその照明器具を電気的に ON/OFF 制御するためのリレーを含む照明回路、これらを統括制御する CPU とそれにクロックを供給するタイマー、これらに電源を供給する電源回路から構成される。図 1 にこの昼光センサ付照明システムの外観イメージとブロック図を示す。

本システムに対する当初の要求仕様は「昼間は消灯しており、夜間は点灯して周囲を明るく照らす」である。

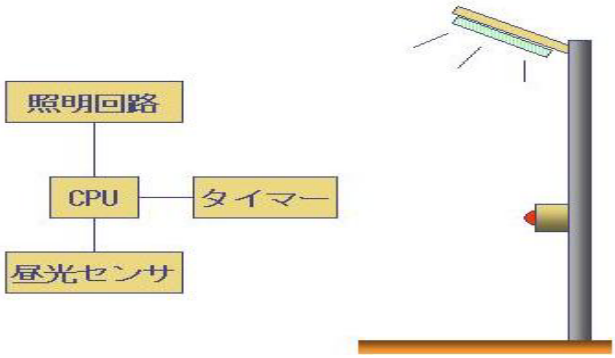

図 1：昼光センサつき照明システムの事例

以下、分析の結果得られた事項について述べる。

1－パッケージ系ソフトと組込みソフトでは、非正常現象発生の主要なトリガが異なる

非正常現象の概念自体は組込みソフト固有の概念ではない。しかし組込みソフトにおいては、パッケージ系ソフトではあまり考慮されない、利用環境からの影響が重要な位置を占めるのが特徴である。屋外で稼動する事による汚れ、風雨などの影響は言うに及ばず、システム利用者でない人間が意図せず組込みシステムの動作を妨害する事なども考慮しなければならない。例えば、昼光センサ付照明システムにおいては、先の雨風及び天候のほか、夜間にヘッドライトを点灯した自動車が通りかかった場合や子供のいたずらの可能性も考慮しなければならない。また、部品の故障や機能の劣化へもある程度対応しなければ可用性の高いシステムとして市場に受け入れられない。更に、ハード的な設計によっては、夜間にシステム自身が照明を点灯した事でセンサはこれを昼間の明るさと判断してしまう可能性もある。これらはモデリングに際してシステムのアクタを決定する場合、一般的なイメージであるアクタはシステムの外部にあるもの、との考えを改める必要性を意味している。即ち組込み系では周辺環境もシステムと同時にモデリングする必要がある。

2－実装技術によって発生する非正常系が決まる

システムにおいて発生しうる非正常現象の種類は、そのシステムにおける実装技術に依存して決定する。例えば昼光センサ付照明システムでは、夜間にヘッドライトを点灯させた自動車が通過するといったケースを想定する必要が生じる。一方、システムクロックを採用したシステムにおいてはこのケースを想定する必要はなく、代わりに実際の時刻とシステムクロックの時刻の不一致を考慮する必要が生じる。

このことは、組込み系においてはハード/ソフトの設計が、仕様に影響を及ぼす事を意味している。このことから、システムの実装技術を決定する事で、それに伴う非正常現象が形式的に導出できる事が期待される。

3－非正常現象の伝播

システム内で発生した現象が、別の非正常現象の原因となることがある。例えば、昼光センサ付照明システムにおいて、システムが夜と判断して照明を点灯した結果、その光をセンサが検知して昼と判断する、といった異常

や、明け方や夕方など、明るさが安定しない状況下では昼光センサからの電圧信号が頻繁に ON/OFF 変化する事が予想されるが、それが CPU の電圧信号検知の割り込み処理の頻発につながるといったことが挙げられる。このことは、システムの動的側面を考慮して分析を行う必要がある事を表している。このような現象の伝播は組込みソフト分野に限った現象ではないが、組込みソフト分野においてはハードや OS、ミドルウェアといった階層も仕様分析段階で考慮に入れる必要があるため、分析が困難となる一因となっている。

４－ハードの非正常発生の検知をソフトの機能として求められる事が要求される

コスト要求の厳しい組込みシステムにおいては、ハードの非正常検知を行うために高価な部品を用いたり、非正常検知用の回路を設ける事を最低限に留めるために、ソフトによってハードの非正常検知を行う事が要求される事が多い。

５－1 つの非正常現象に対して、複数の対応手段が存在する

ある非正常現象を検知した場合、システム、サブシステムあるいはコンポーネントは以下のような処理をとる事ができる。１：非正常の原因を取り除く、２：非正常の発」生を外部に通知する、３：時間経過による非正常からの回復を待つ、４：非正常現象発生箇所をシステムから切断し、影響の拡大を防ぐ。また、これらの処理と並行して、次善手段を採用する事もできる。例えば昼光センサ付照明システムにおいて昼光センサからの入力信号がめまぐるしく変化して昼夜いずれとも判断し難い場合（センサの故障が原因）の対応方法について、前述の種別毎に考えると、1 はソフトでの実現は困難、2 は異常通知 LED などによってメンテナンス者への注意を促す方法、３はある程度時間を置いて、センサからの入力信号が安定するまで待つ方法、４は昼光センサを昼夜の判断基準から外す方法、次善手段は例えばタイマによって 12 時間毎に昼/夜を区別するといった方法がそれに相当する。

６－非正常への対応手段の利用可否は実装技術に依存する

先に、1 つの非正常現象に対して複数の対応手段がある事について述べたが、システムの実装技術によっては採用できない対応手段が存在する。先の例では、非正常の原因を取り除く対応は、例えば昼光センサを自動的に交換する機能をシステムに設ける事に相当するが、その対応は現実的ではない。また、コスト削減のために異常検知 LED を実装しないとすれば、外部への通知方法は別の方法に依るか、通知しないとする仕様に変更する必要がある。

７－非正常への対応手段は、要求仕様における優先順位付けによって決定される

１つの非正常現象に対して複数の対応手段が取りえる場合、各手段のうちいずれを選択するべきかの判断基準は、システムの要求仕様における優先順位に委ねられる。昼光センサ付照明システムの場合、昼光センサの故障時に照明をどのように制御するかの仕様は、もしそのシステムが安全性を重視したものであれば ON 制御する事が、もしそのシステムが省エネルギー性を重視したものであれば OFF 制御する事が望ましいと判断される可能性がある。段落にまとめる.

以上に示したように、非正常現象は様々な情報と関連を持つが、そのうち非正常系仕様の検討に先立って与えられる事が多い情報として、システムでの実装技術（特にハード）が挙げられる。このことから、システムの失上技術とそれに伴って生じる可能性のある非正常現象との関連を中心に知識体系を構築し、その知識体系に開発対象システムの採用手段を入力として与えることで、開発対象システムで発生しうる非正常現象とその対応方法を出力とするような開発者支援システムを構築できる事が期待される。

３．非正常系の概念モデル

前章にて、開発対象システムでの実装技術とその実装技術に応じて発生する非正常現象との関連を中心に知識ベースを構築する事で、仕様分析段階の支援可能であるとの仮説を得た。そこで我々は、知識ベース構築のため、非正常系仕様抽出のための組込みシステムの概念モデリングを行った。本章では、そのモデルについて示す。

３.1　モデリングのスコープ

組込みシステムは環境との関係が非常に深い。それはパッケージ系ソフトは利用される環境における人間が占める比率が高いため、人間の判断によってシステムへの影響をコントロールする事ができるが、組込みシステムは利用される環境における人間の占める比率が低く、時には無人環境での動作を要求されるためである。このような理由から、組込みシステムの概念モデリングにおいては、システムが置かれる環境も含めたモデリングが必要である。

３.2 情報フロー・ダイアグラム

例として、昼光センサ付照明システムにおいて、システムは「昼/夜」と判断するための情報をどのように得ているかについて考察する。この場合、システムは昼光センサが受光する光の、光の量によって昼夜の区別を行っている。即ち、システムは光の量によって「昼/夜」の情報を受け取っている。この光は発光する物体から直接、もしくは光を反射する物体を経由して、空間の中を通過してくる。また、光の量という情報の運び手によって運ばれた「昼/夜」の情報は、昼光センサにて銅線の中を通過する電気信号によって CPU まで運ばれるようになる。この事から、昼光センサは情報の運び手を光の量から電圧信号に変換させる役割を担っていると言える。

以上の考察から、システム及びそれを取り巻く環境について、以下のように定義する。

・システムに関連する情報の運び手をキャリアと呼ぶ。例えば、昼光センサに対して「昼/夜」の情報をもたらす光の量はキャリアである。

・キャリアの送信元を情報発信者と呼ぶ。

・キャリアの経路を情報フローパスと呼ぶ。例えば、電圧信号の経路である銅線は情報フローパスである。

・キャリアを変換する物を情報変換ポイントと呼ぶ。例えば、昼光センサはそれまで光の量というキャリアが運んできた「昼/夜」という情報を、電圧信号に運ばせるようにするため、情報変換ポイントと呼ぶ。また、情報変換ポイントは、変換後のキャリアの受信側から見れば情報発信者と言える。

３.3　非正常系の発生

前節で示した定義に基づいてシステムに情報がもたらされる仕組みをモデリングした場合、非正常現象の発生は情報発信者、情報フロー、情報変換ポイントにて発生するものとする事ができる。情報発信者において発生する非正常現象をなりすましと呼ぶ。なりすましとは、情報受信者（情報変換ポイント）が受信する情報を、本来発すべき情報発信者以外の発信者が発信している現象を表す。例えば、昼光センサは、センサが捉える光の量によって昼あるいは夜という情報を得るが、夜間にヘッドライトを点灯した自動車が昼光センサの近隣を通過する事によって、センサは昼に相当するだけの光を受信する。この場合、昼という情報を、本来の情報発信者である太陽ではなく、自動車のヘッドライトが太陽になりすまして発信していると言える。また、情報フローにおいて発生する非正常現象を、ここでは情報フローパス妨害と呼ぶ。情報フローパス妨害は、情報のキャリアが通る情報フローパスに情報のキャリアの通過を妨げるものが現われる現象を表す。例えば、昼間であっても、センサの前

に光をさえぎる障害物が置かれた場合、センサに入る光の量が減少してセンサは夜という情報を得てしまう。
次に、情報変換ポイントにて発生する非正常現象を、ここでは情報変換ポイント例外と呼ぶ。情報変換ポイント例外は、情報変換ポイントの特性が変化した結果、変換前と変換後の持つ情報が変化する現象を表す。例えば、昼光センサの受光回路が経年劣化などで当初より多い量の光を受光しないと昼と判断できないようになってしまった場合、この昼光センサにて情報変換が行われる前と後で、昼という情報が夜という情報に変わってしまう事がある。
このように、システム及びそれを取り巻く環境で発生する非正常現象は、情報フロー・ダイアグラムの概念の上では、以上の 3 種類に分類する事ができる。

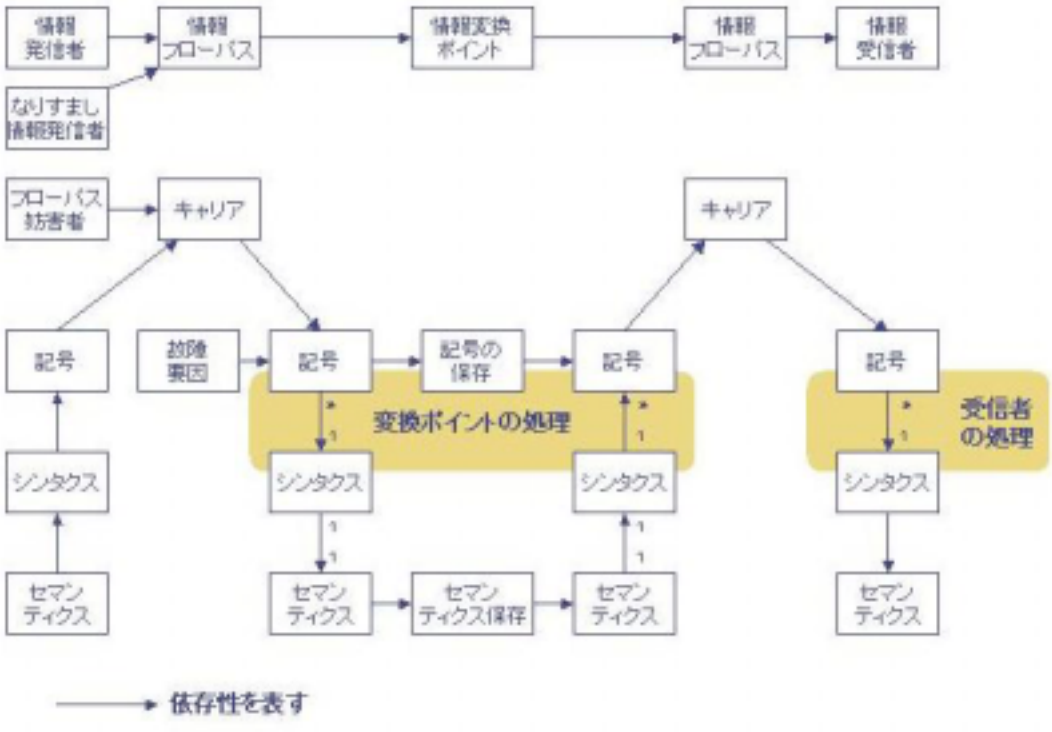

図 2：非正常系の概念モデル

3.4 非正常現象の概念整理の枠組み

前節で示した情報伝達の基本的モデルと非正常現象の発生を反映した情報伝達の概念整理の枠組みを図 2 に示す。同図では、情報発信者と情報受信者が情報フローパスと隣接しており、その情報はやはり情報フローパスと隣接している情報変換ポイント変換される事が表されている。情報は、情報発信者から発信され、フローパスの中を伝達して途中で何度か変換され、最終的に情報受信者に到達する。また、情報のキャリアについては、そのキャリアが情報フローパスの中で果たす機能によって情報を伝達する事に着目している。キャリアが果たす機能がどのように情報を伝達するかについては、情報の表現階層である記号・シンタクス・情報の各レベルを用いて表現する。図 2 のモデルを用いて、事例である昼光センサ付照明システムにおいて発生しうる非正常系現象について記述すると、図 3 のようになる。

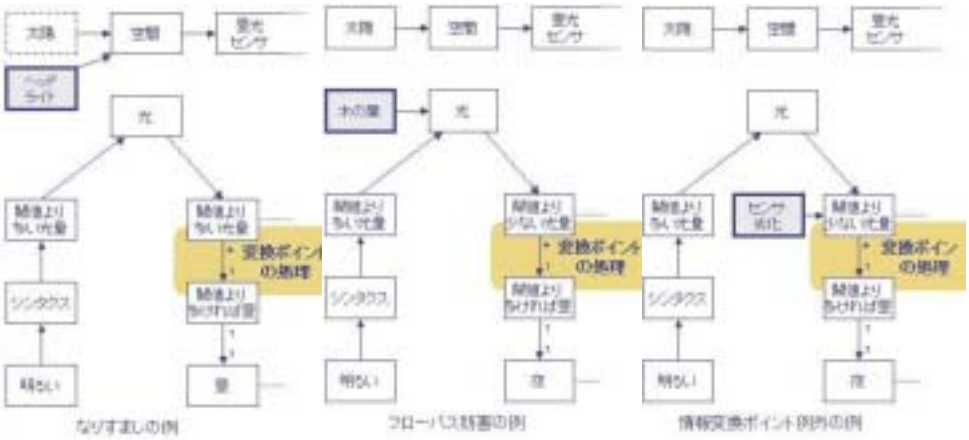

図 3：非正常現象の事例

４．考察

前章で示した非正常系概念モデルが、どの程度の一般性を持つかについて考察する。まず、本モデルの根幹をなす情報フローパスの概念についてであるが、本モデルは“情報発信者-フローパス-情報変換ポイント-フローパス-情報受信者”と情報伝達に関して一般化された概念で構成されている事、本モデルがシステムと周辺環境を含んだモデルになっている事、どんなに内部構成が単純なシステムであっても、最低限周辺環境との間に情報伝達を行う事から、本モデルはシステムにおける一般性を保持していると考えられる。

次に、本モデルにおける 3 種類の非正常現象の妥当性についてであるが、これについては本モデルの根幹である、情報発信者からフローパスを通じて受信者（情報変換ポイントも含む）に伝わるまでの過程における問題を、やはり情報伝達を用いる概念であるネットワークセキュリティの分野における危険性と比較する事で説明可能である。本モデルにおける情報発信者へのなりすましはネットワークセキュリティ分野のそれと同じ事が言え、情報フローパス妨害はネットワークセキュリティ分野における情報の改竄に相当する。また、情報変換ポイント例外は、誤用に相当すると考えられる。ただしネットワークセキュリティ分野における危険性として、盗聴、使用拒否、乱用、否認に相当する非正常現象は直接的に対応する現象が存在しない。このうち盗聴は、システムの外部環境をシステムと区別する場合に考慮すべき危険性であるため、外部環境を含めてモデル化した今回のモデルでは、異なる概念で取り扱うことがふさわしい。また、使用拒否、乱用、否認は情報の伝達そのものではなく、情報の伝達を利用したサービスのレベルで考慮すべき問題である事から、このモデルでは対応すべき概念が存在しないと考えられる。以上のように、本モデルの根幹となる概念のうち、直接情報伝達に関わる危険性はモデル内に網羅されていることから、本モデルの概念が環境的ドメインに依存せず一般に適用可能であると判断される。

５．今後の課題とまとめ

本稿では、非正常系仕様の記述において考慮すべき事項についての事例分析結果について述べ、その結果から、非正常系仕様の知識ベース化と仕様言語記述による支援が可能であるとの仮説を立てた。さらにこの仮説に基づ

き、非正常系仕様の知識ベース化を目的として作成した非正常系の概念モデルを提示した。また、このモデルがソフトウェアの環境に依存しない一般的な概念表現が可能であるかについて考察した。

我々は、組込みソフトの仕様記述支援システムを以下のような構成で構築する事を検討している。支援システムではまず、要求者が正常系仕様及びハード要件などの記述を行う。この記述及び非正常仕様知識ベースから抽出された知識を用いて非正常仕様を自動生成する。最終的に正常系仕様と非正常系仕様の記述を合成し、開発対象システムの全体仕様とする。このようにして仕様記述支援を実現する。構成するシステムを図 4 に示す。

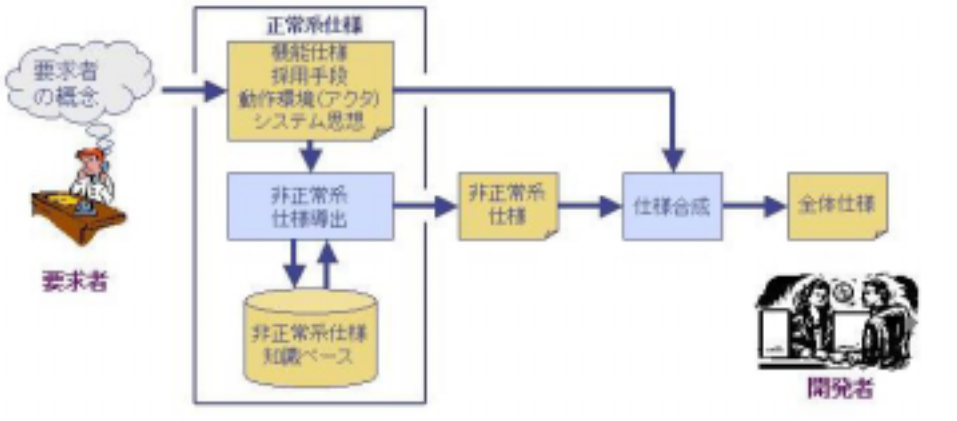

図 4：仕様設定支援システムの概念図

上記支援システムを実現するためには、今後の研究で以下の課題を解決する事が必要である。

- 本論文で提示した概念モデルの検証
- 概念モデルを元にした非正常仕様知識ベースの構築
- 正常系仕様と非正常系仕様の合成が可能な仕様記述言語の定義

今後は実際のソフト開発への適用を交え、上記課題の解決を図る。

参考文献

[1]経済産業省 ”2004 年版組込みソフトウェア産業実態調査報告書”

[2]江浦洋平、畑中久典、橋本正明 “事例に基づく組み込みシステムの非正常系事象モデルの研究”、九州工業大学大学院情報工学研究科 2003 年度修士論文

[3]渡辺博之、渡辺政彦、堀松和人、渡守武和記 “組込み UML”、翔泳社

[4]野村昌男、久保秋真、伊藤恵、片山卓也 “組み込みシステム設計のための ObTS に基づく記述支援環境に関する研究”、情報処理学会ソフトウェア工学研究会研究報告 No.125-13,2000

[5] **F. Casati and G. Cugola, “Error Handling in Process Support Systems”, Advance in Exception Handling Techniques, LNCS 2022, pp.251-270, 1998**