Special edition paper

信号保安ソフトウェア品質向上に向けた要求分析手法の研究

Study of Requirements Analysis Method for the Signaling Safety Software Quality Improvement


安倍　孝典*


寺本　学**


岡田　明正*


福田　和人*

Signaling safety software becomes complex by the ICT (Information and Communication Technology) advancement of the signaling safety system. Therefore, the importance of the requirement specifications to be incorporated into the signaling safety software is increasing. In this study, we provided a requirements analysis template to prevent definition omission or error of the requirements specification. Quality improvement requirements specification by using the request analysis template is expected.

●キーワード：信号保安ソフトウェア、信号保安システム、要求分析、要求獲得、要求定義

1. はじめに

ICT（Information and Communication Technology）の進展により信号保安システムの高度化が進んでいる。それに伴い、信号保安ソフトウェアの重要性も増しており、高い品質が求められている。一般に、ソフトウェア開発の上流フェーズに位置するソフトウェア要求仕様フェーズの品質は下流フェーズの品質に大きな影響を及ぼす。そのため、ソフトウェア要求仕様フェーズの品質向上はソフトウェア全体の品質向上に繋がることが期待できる。

本研究では、国際規格IEC 62279[1]に示される開発ライフサイクル（図1）のソフトウェア要求仕様フェーズを対象とし、ソフトウェア要求分析の品質向上を目指すための手法について取り上げた。ソフトウェア要求仕様フェーズで定義される要求の質を高めることで信号保安ソフトウェアの品質向上を目指す。

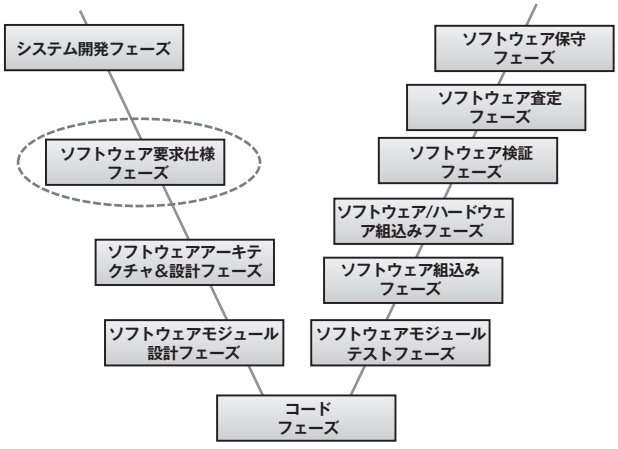

図1　IEC 62279に示される開発ライフサイクル

2. 現状の把握

2.1　信号保安ソフトウェア仕様の課題

信号保安システムの高度化により、信号保安ソフトウェアが大規模化・複雑化している。それに伴い、信号保安ソフトウェア開発において、仕様の漏れや認識齟齬によるソフトウェア品質の低下が懸念されるようになった。そこで、要求仕様策定に関する種々の課題について具体的な整理を行った。

その結果、下記の点が信号保安ソフトウェアのソフトウェア要求仕様フェーズに関する課題として集約された。

(1) 仕様の定義漏れ

ユーザにとって自明である暗黙知の要求が漏れ、下流工程になって判明する。

(2) 仕様の関連が不明確

要求や仕様の関連が不明確なため、仕様変更時にその影響範囲が特定できない。

2.2　信号保安ソフトウェア仕様の特徴

課題に対する解決方針を定めるため、ユーザ・メーカにて「ブレーンストーミング」、「過去の仕様検討資料確認」、「制御図表・結線図から仕様読み取り実験」を行い信号保安ソフトウェア仕様の特徴を洗い出した。以下に抽出された特徴を分類した結果を示す。

(1) 安全性・信頼性等非機能要求が多い
(2) 既存仕様である制御図表・結線図の確認では認識に齟齬が出る
(3) 要求の抽象度にバラつきがある
(4) 様々な列車の動きを踏まえた仕様が策定される
(5) 派生機種が多く、それに伴う仕様の変更が多い

*JR東日本研究開発センター　先端鉄道システム開発センター
**東北工事事務所　（元　先端鉄道システム開発センター）

2.3 課題解決の方針

課題と信号保安ソフトウェア仕様の特徴の関係を整理した（図2）。すると、信号保安ソフトウェア仕様の特徴が課題を引き起こす原因となっていることが分かった。そこで、課題の原因となっている特徴を考慮しつつ課題解決の方針を定めた。以下に課題解決の方針を示す。

（1）仕様の定義漏れ（図2 課題①）

・暗黙知的な要求、特に非機能要求を漏れなく定義（図2 解決方針①）

・現行システムを分析し、その結果を明示（図2 解決方針②）

・様々な列車の動きを踏まえた仕様を定義し、またその結果を明示（図2 解決方針④）

（2）仕様の関連が不明確（図2 課題②）

・仕様の導出根拠に関する関係を明示（図2 解決方針③）

課題解決の方針の結果をもとに、信号保安ソフトウェアの要求分析手法を検討することにした。

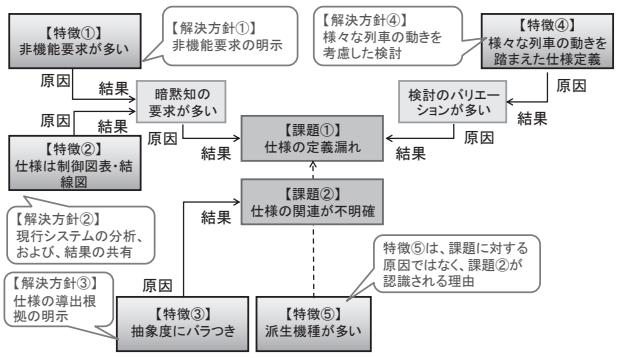

図2 課題と信号保安ソフトウェア仕様の特徴の関係性

3. 要求分析手法

3.1 要求分析テンプレートの策定

一般に、通常の打合せと同様、要求分析作業は口頭打合せ、文書のやりとり等で実施する。この際、業務知識や経験の多寡によって、要求の抜けや粒度のバラつき、理解の齟齬が発生するのは不可避であった。そこで要求分析作業の定型化をねらい要求分析テンプレートの策定を検討することにした。

要求分析テンプレートでは、「仕様の定義漏れ（図2 課題①）」については、要求分析時の検討観点を明示化することで仕様の定義漏れを防止すること、「仕様の関連が不明確（図2 課題②）」については、仕様と、その導出根拠である要求との関連を明確にすることを目指した。

その上で、要求分析テンプレート策定の方針と活用可能な既存手法について検討し、整理を行った。表1に整理した結果を示す。この結果をもとに「要求分析テンプレート」の内容を考案した。

要求分析テンプレートは、要求分析時に検討すべき各種項目を示したもので、それらに対する検討結果をユーザ・メーカがそれぞれ書き込むことができる。図3に要求分析テンプレートの構成を示す。

表1 要求分析テンプレート策定の方針

課題解決の方針		課題解決へのアプローチ	活用可能な既存手法
仕様定義の漏れ		全体的な仕様定義漏れを防ぐために、要求分析テンプレートを策定	IEEE 830–1998[2]要求仕様書テンプレート
	暗黙的の要求、特に非機能要求を抜け漏れなく定義	テンプレート内に非機能要求を分析する節を設け、具体的な非機能要求をの観点を列挙する	ISO/IEC 9126[3]、25010[4]ソフトウェア品質モデル
	現行システムを分析し、その結果を明示	テンプレート内に現行システムに関する分析を行う節を設ける	表現方法として、UML[5]、DFD[6]等
	様々な列車の動きを踏まえた仕様を定義し、またそれを明示	テンプレートにおいて、仕様検討のための枠組みの提示および時間軸に沿った列車の動きを表現するための記法を検討する	タイミングチャート
仕様の関連が不明確		関連を分類し、それぞれに応じた表記方法を検討	ゴールツリー[7]、USDM[8]、DFD等関連の種別に応じて
	仕様の導出根拠に関する関係を明示	仕様の導出根拠については、特にテンプレートのフォーマットとして記載されるようにする	ゴールツリー、USDM

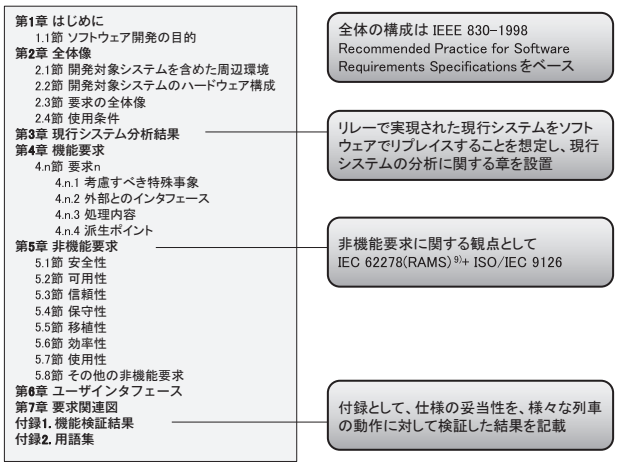

図3 要求分析テンプレートの構成

要求分析テンプレートの特徴は、信号保安システムの仕様に適した検討項目の構成になっており、要求から仕様への導出過程を記録するフォーマットとしている点である。

仕様と、その導出根拠である要求との関連を示すフォーマットとして従来からUSDM（Universal Specification Describing Manner）という記述方式が提案されている[8]。要求分析テンプレートでは、USDMの記述方法を拡張し、要求の分析の検討過程や仕様決定理由を記載するフォーマット（図4）とした。これにより、要求から仕様が導き出された導出過程・理由が明確になる。

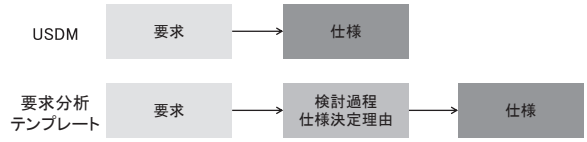

図4 要求分析テンプレートによるUSDMの拡張

具体的には、要求分析の過程として、要求に関する質疑を記録し、それを踏まえた仕様決定の理由および結論を記載する。なお、仕様そのものについては、機能仕様書の記載と重複を考慮して、要求分析テンプレートには記載せず、

機能仕様へのリンクを示す形式とした。また、ユーザが記載する欄とメーカが記載する欄を分離することにより、両者それぞれの考えが明確に示されるための工夫を行った。

その他、特徴として要求分析テンプレートの各章ごとに記載内容、記法等に関するガイドラインを記述することにした。

3.2 要求および仕様の関連の表記法

一般に、要求や仕様の関連には図5に示すように、以下の3種類があるが、従来の信号保安システムの開発ではこれらの関連の違いに対する考慮が十分ではなかった。

(1) 要求−仕様間の関連
(2) 要求−要求間の関連
(3) 仕様−仕様間の関連

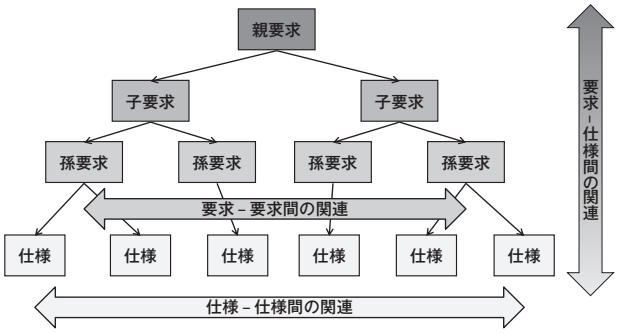

図5 要求および仕様間の関連

要求および仕様の関連の表記法として、要求−仕様間の関連は、要求分析テンプレートのユーザ記載とメーカ記載の区分によるUSDMの拡張フォーマットで表記できる。しかし、関連はそれだけではない。図5に示されるように要求−要求間の関連や、仕様−仕様間の関連がある。これらの関連の表記法について検討を行った。

その結果、要求−要求間の関連については、目的−手段の関係にある関連も含めて、ゴール指向分析で用いられるゴールツリー（図6）で表記することが適切である。

仕様−仕様間の関連については、特に機能間の関連の表記が重要となる。これを表現するには、構造化分析手法で用いられるDFD（Data Flow Diagram）（図7）で表記することが適切である。

以上をまとめると、要求や仕様の関連の種別に応じて、それぞれ表2の表現方法による使い分けが望ましい。これらの利用可能な表記法を、要求分析テンプレートに取り入れた。

3.3 拡張タイミングチャート

信号保安システムの仕様は、様々な列車の動きに対して妥当であることの検証が欠かせない。検証結果として、列車の動きに同期して入出力信号がどのように振舞うか表現する記法が求められる。

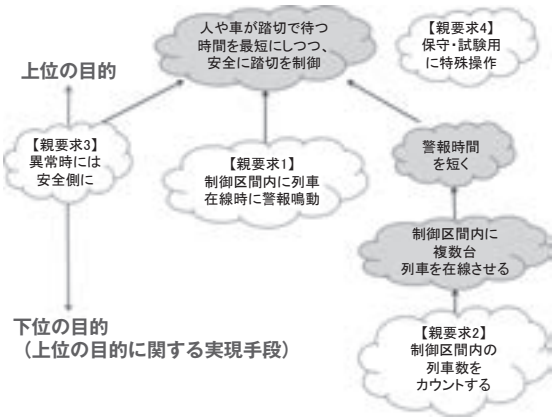

図6 ゴールツリーを用いた記載例

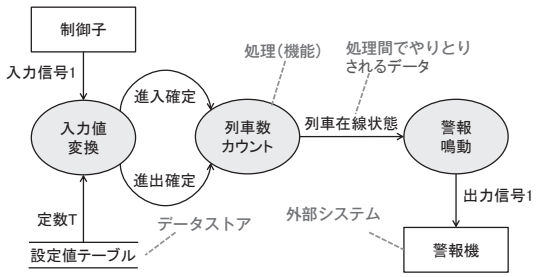

図7 DFDを用いた記載例

表2 関連の表現

関連の種類	関連の表現方法
要求-仕様間	要求分析テンプレート中のUSDMの拡張フォーマットにて表現
要求-要求間	親子関係にある要求-要求間の関連も含めて、ゴールツリーにて表現。ゴールツリー上で関連する要求-要求間の関連を線で繋ぐ
仕様-仕様間	仕様-仕様間の関連をDFDにて表現

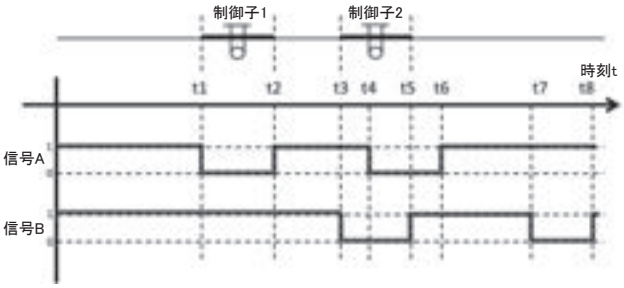

図8 タイミングチャート

時間軸に沿った信号の変化を示すための記法として従来からタイミングチャート（図8）がある。タイミングチャートでは横軸に示した時間軸にそって、各種信号の値の変化を示している。現状の信号保安システムの機能仕様書では、これに位置に関する情報を重ねて、列車の動きに対応付けた振舞いを表現しようとしている。図8では、列車が左から右に進行し、時刻t1で制御子1の検知区間に差し掛かり、それに伴って制御子1の信号Aが1から0に変化する。その後、時刻t2で制御子1の区間から抜け、信号Aが0から1に戻ることを表している。この表記法でも一つの列車の一定速度での進行

に対応した信号の振舞いは十分表現できている。

しかし、この表現方法では複数の列車・列車長・速度に関する表現に問題がある。図8において、信号Aが時刻t4において1から0に変化する理由は、この図を見ていても理解できない。実はこの図では続行列車の動きを示している。時刻t4での信号Aの変化は続行列車によることを示しているのである。また、時刻t1にて制御子1の信号Aが1から0になった時は、列車の先頭が検知区間に差し掛かったこと示している。一方、時刻t2にて信号Aが0から1になった時は、列車の後端が検知区間から抜けたことを表している。これらについて、図8から正確に理解することができない。

このような問題を解決するため、時間軸と位置に関する軸を明確に分離した「拡張タイミングチャート(図9)」を定義した。

拡張タイミングチャートでは、位置に関する情報を時間軸に直行する形で表現し、時間軸と位置軸の座標上で列車の動きを表現している。図9では二つの列車の各時刻における位置が明確に示され、列車と信号の関連が可視化されたことで時刻t4での信号Aが1から0に変化した理由が二本目の列車だと分かる。

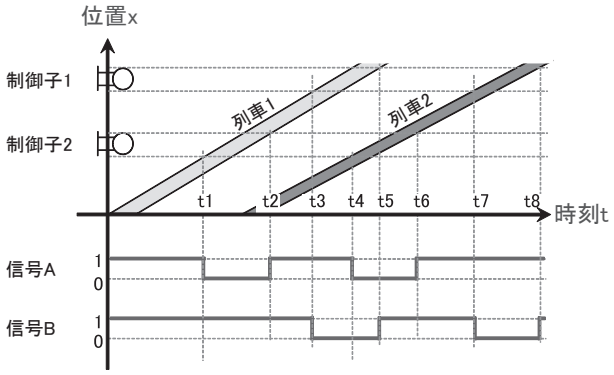

図9　拡張タイミングチャート

列車を表す線には幅を持たせており、これは列車長を表している。これにより列車の先頭が制御子の検知区間に差し掛かったタイミングや列車の末尾が制御子の検知区間から抜けたタイミングが表現できる。また、列車を表す線の傾きにより列車の速度も表現できる。

利用可能な記法の提案として拡張タイミングチャートを要求分析テンプレートに取り入れた。

4. 今後に向けて期待される効果

要求分析テンプレートの活用により以下の効果が期待される。

要求分析テンプレートは、ユーザ記載、メーカ記載箇所が明確に分かれているため、両者の考えが明確になる。特に、要求分析の最初にユーザが提示する要求については、これまで明確なフォーマットがなく開発者により多種多様の形式であったが、要求分析テンプレートがあることにより初期提示内容の充実ができ、手戻りの削減に繋がることが期待できる。

要求や仕様の関連については、仕様はすべて要求に紐づけられた形で要求分析テンプレートに記載するため、導出根拠は明確になる。要求同士、仕様同士の関連については、ゴールツリーやDFD等の表現により、要求の可視化ができ、こちらについても手戻りの削減に繋がることが期待できる。

拡張タイミングチャートについては、具体的な列車の動きを明示できるため複雑なケースに対する検証結果が適切に可視化できる。

これらの効果により、ソフトウェア要求仕様フェーズの品質向上が期待される。

5. おわりに

本研究は、信号保安ソフトウェア開発におけるソフトウェア要求仕様フェーズの要求分析プロセスの改善を目的として「要求分析テンプレートの策定」、「要求および仕様の関連の表記法の検討」、「拡張タイミングチャートの提案」を行った。これらによりソフトウェア要求仕様フェーズで定められる要求の品質は大きく向上し、その結果、信号保安ソフトウェアの品質向上に繋がると期待される。

今後の課題として、要求分析作業に対するより緻密なサポート、各種記法の習熟、システム要求分析を含めた開発プロセスの整理が挙げられる。

今後は、試行的に要求分析テンプレートを用いた仕様策定を行い、モデルケースにて評価する予定である。

参考文献

1) IEC 62279 Ed. 1.0 : Railway applications - Communications, signalling and processing systems - Software for railway control and protection systems, IEC (2002)
2) IEEE Std 830 : Recommended Practice for Software Requirements Specifications, IEEE (1998)
3) ISO/IEC 9126-1 : Software engineering - Product quality - Part 1:Quality model, ISO/IEC (2001)
4) ISO/IEC 25010 : Systems and software engineering – System and software product Quality Requirements and Evaluation (SQuaRE) – System and software quality models, ISO/IEC (2011)
5) Unified Modeling Language (UML), http://www.uml.org/, OBJECT MANAGEMENT GROUP (2013.2.6)
6) 細谷僚一・斎直人:「構造化分析設計技法入門」, 電気通信協会 (1996)
7) 山本修一郎:「要求工学基礎知識」, 名古屋大学 (2012)
8) 清水吉男:「要求を仕様化する技術・表現する技術」, 技術評論社 (2010)
9) IEC 62278 Ed. 1.0 : Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS) , IEC (2002)