# オブジェクト指向開発手法の信号保安装置への適用の研究



国藤　隆*　　加藤　尚志*　渡邊　貴志*

当社においては、信号保安装置の電子化施策を積極的に展開しており、連動装置に着目すると５０％の駅がソフトウェアで制御されていることになる。また、従来の信号制御、踏切制御の枠組にとどまらず、保守作業管理機能の搭載など多機能化も進んでいる。この傾向は今後とも拡大の一途をたどるものと思われ、保安ソフトウェアの生産性、保守性の向上は喫緊の課題である。しかしながら保安ソフトウェアの開発プロセスには、高度な安全を作りこむための制約が多く、世の中一般のソフトウェア生産性向上に寄与している新技術の採用には十分な検証が必要である。そこで本稿ではオブジェクト指向開発手法を信号保安装置へ適用するに当たっての課題と指針を示す。

●キーワード：オブジェクト指向、信号保安装置、UML、ソフトウェア開発プロセス

## 1　はじめに

近年、信号保安装置の制御論理のソフトウェア化、およびそれを実行するプラットフォームの汎用機化が急速に進展している。また信号保安装置に求められる機能も多様化しており、ソフトウェアの役割は増大する一方である。したがって、高品質のソフトウェアを短期間で開発する手法の整備は喫緊の課題である。

ところで、PC向けのソフトウェア開発においては、オブジェクト指向技術の利用が一般化し、デザインパターンに代表される、再利用可能なソフトウェア部品の設計技法、CORBA等の分散オブジェクト技術が確立しソフトウェアの、生産性向上、品質向上に大きく寄与している。また、これらオブジェクト指向技術は、信号保安装置に比較的アーキテクチャが似通ったリアルタイム制御向けの機器組み込みソフトウェアの分野での活用も進展している。

そこで、オブジェクト指向技術の保安制御ソフトウェア開発への適用を電子踏切制御装置を対象にして試行し、有効性の検証、及び課題抽出を行った。

## 2　保安ソフトウェア開発の課題

保安ソフトウェア開発の現状を分析すると、以下に示す課題が抽出された。

(1) 個人の経験に依存する部分が大きい

リレー制御方式の信号保安装置における標準結線図に相当するソフトウェア設計ノウハウが整備・蓄積されておらず、過去の特定の保安ソフトウェアの開発で得られた経験的知識をもとに設計を行う傾向にある。

(2) ユーザとメーカー間での意思疎通が十分でない

ユーザ側とメーカー側の開発担当者の技術背景にミスマッチがあり、仕様の共通理解が十分に行われず、結果として手戻りや不具合として表面化する

(3) 多機能化要望による変更頻度の増大

従来人間系の注意力により行われていた部分も、信号保安装置の機能として実現が求められる傾向にあり、保安ソフトウェアの変更頻度は増大している。

これらは、保安ソフトウェアの品質向上を阻害する要因であり、その解消に向けて開発プロセスを策定し、開発フェーズごとに作成すべきドキュメントを規定するなど、システマティックなアプローチが必須であると考える。それにあたっては、最新のソフトウェア構築技術の適用を図るとともにソフトウェア安全性規格への適合性検討が必要と考える。

## 3　オブジェクト指向開発手法

### 3.1　オブジェクト指向とは

「オブジェクト指向」とは、人間が物事を認識するのと同様のやり方でシステム化対象をコンピュータ上に抽象化して表現する概念や技術の総称である。この抽象化された対象物をオブジェクトと呼び、オブジェクト自身の振る舞い、分類、及び構造、またオブジェクト間の相互作用を定義することによってシステムの動作を表現するものである。

*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

### 3.2 オブジェクト指向のメリット

一般にソフトウェアの品質は以下の観点で計られるがオブジェクト指向はこれらの品質要因を向上させることのできるソフトウェア工学に裏づけされたアプローチである。

(1) 正確さ

ソフトウェア製品が要求及び仕様によって定義されたとおりに確実に仕事を行う能力

(2) 頑丈さ

異常な状態においても機能するソフトウェアシステムの能力

(3) 拡張性

ソフトウェア製品が仕様の変更に容易に適応できる能力

(4) 再利用性

あるソフトウェア製品の一部分が、どの程度新しいアプリケーション構築に再利用できるかを示すもの

(5) 互換性

あるソフトウェア製品相互の組み合わせやすさ

保安ソフトウェアにおいては、安全性の観点から、正確さ、頑丈さが絶対的な優先事項であることは当然であるが、保安装置であっても多機能性が求められることから、それ以外の品質要因の重要度も増してきている。

### 3.3 オブジェクト指向による分析・設計手法

オブジェクト指向による分析・設計の特徴は、システム化対象を、従来のように機能中心ではなく、データ構造中心にモデル化していくアプローチにある。これは、システムが取り扱う対象すなわち、データの構造は機能に比べて長期的には普遍であり、再利用性、拡張性の向上に有利であるという理念にもとづく考え方である。

#### 3.3.1 UMLによるモデリング

オブジェクト指向によるモデル化のプロセスでは、UML（Unified Modeling Language／統一モデリング言語）と呼ばれる表記法が用いられる。UMLは1997年にOMG（Object Management Group）により標準化されデファクトスタンダードとなっている。

UMLではシステム化対象を「実現すべき機能」、「静的な構成」、及び「動的な振る舞い」の３つの側面から分析し、それらをグラフィカルに表現する表記法が定められている（図１）。グラフィカルな表記を用いることでユーザとメーカーとの間でシステムに対する知識を共有することが容易となる。また、システム開発の最初から終わりまでを共通のUMLドキュメントを用いてシームレスに行うことができ、首尾一貫性が保たれる。

#### 3.3.2 再利用技術

オブジェクト指向の利点の一つに再利用性の向上がある。再利用は、要求分析からコーディングにいたる、すべての工程で可能であり、再利用可能な部品をパターンとしてまとめる技術が提唱されている。また、パターンの記述にもUMLを用いることができる。以下に代表的なパターンについて説明する。

(1) ドメインモデル

ドメインの知識をモデル化したもの

(2) アーキテクチャパターン

典型的なソフトウェアアーキテクチャを記述したもの

(3) アナリシスパターン

オブジェクト指向分析段階でオブジェクトをモデリングするための指針を表現したもの

(4) デザインパターン

オブジェクト指向設計段階で再利用性の高いオブジェクト構造を実現するための指針を示したもの

(5) イディオム

特定のプログラミング言語に特化したプログラミングのパターン

#### 3.3.3 安全性技術のパターン化事例

信号保安装置自身の安全性の確保は、ソフトウェアとハードウェアの協調動作で行われるため、従来そのソフトウェア部分はハードウェアに依存した特殊処理となっている。これが信号制御の論理を実現する汎用的なアプリケーションと絡み合うことがソフトウェアの保守性が低下する要因となっている。そこで、安全確保の技術をソフトウェア、ハードウェアのコラボレーションとして捉えその構成と振る舞いを分析し、ソフトとハードのインターフェースを汎用的に規定することで再利用可能な安全部品とする

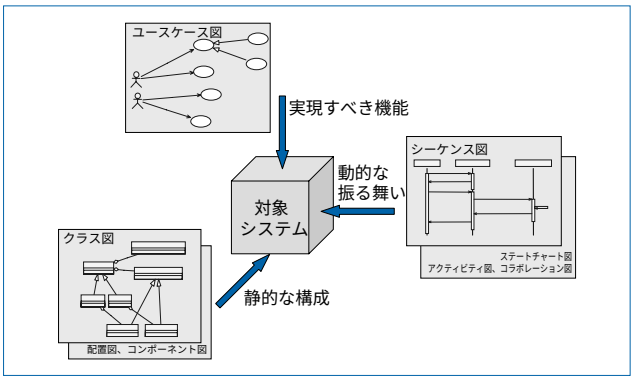


図１：UMLによるモデリングの概念

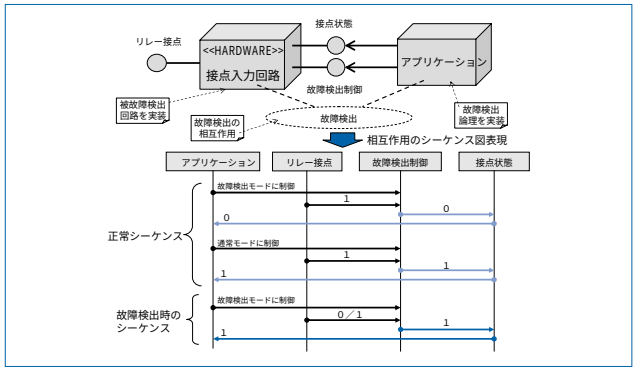


図２：ハードウェアの危険側故障チェックパターン

ことを目指した。

図２にリレー接点を読み出すハードウェアとそのハードウェアの危険側故障を見つけ出すソフトウェアとの相互作用をUMLで表記したものを示す。

### 3.4 保安ソフトウェア開発への適用

保安ソフトウェア開発にオブジェクト指向技術を適用した場合、特に以下の点からの品質向上、及び生産性向上が期待できる。

(1) 仕様に対する共通理解の促進

仕様記述にUMLを利用することで、ユーザ側の信号保安装置の専門家とメーカー側のシステムエンジニアとが共通の言語で対話することができ、技術背景のミスマッチを埋めることができる。

(2) 安全メカニズムの再利用

保安装置に組み込まれた安全メカニズムをパターンとして切り出すことで、標準結線図ともいうべき安全メカニズム集を蓄積していくことが可能と考える。また、パターンの再利用を重ねブラッシュアップされることで、安全性のさらなる向上が見込まれる。

## 4 保安ソフトウェアのオブジェクト指向開発

オブジェクト指向開発手法による保安制御用ソフトウェア開発の試行事例として、踏切をオブジェクト指向で分析し、電子踏切制御装置の設計を行った。その概略について以下に紹介する。

### 4.1 開発プロセス

開発プロセスを策定する目的は、各フェーズでの作業内容と成果物を明確にすることで、仕様、及びその検証の正当性を保証し品質を向上させることである。図３に今回試行した、オブジェクト指向による保安ソフトウェアの開発プロセスをIEC62279に例示された開発プロセスと対比させて示す。

一般に、機能仕様書が出来上がるまでをソフトウェア開発の上流工程と呼び、ユーザとメーカーの共同作業で進められる。一方、それ以降プログラムを設計製作するフェーズを下流工程と呼びメーカー単独作業で行われる。以下に、今回試行した開発プロセスのうち、上流工程で行われる作業とその成果物、及び各フェーズで適用したオブジェクト指向分析手法、安全性解析手法について簡単に説明する。

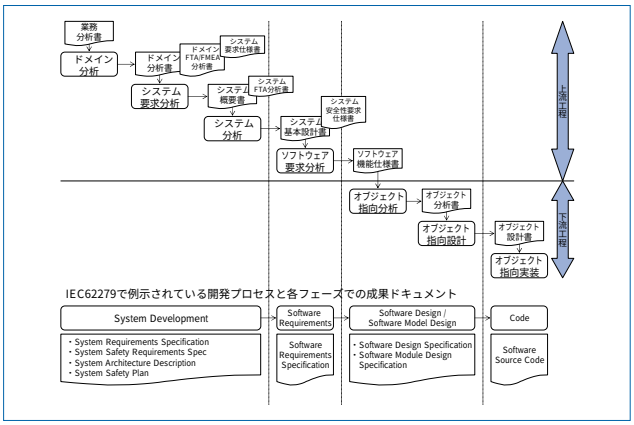


図３：今回試行した開発プロセス

(1) ドメイン分析

ドメイン分析の目的は、ドメインエキスパートであるユーザが保有する知識をメーカーと共有できる形でモデル化していくことである。特に保安制御ドメインには、実施基準、標準結線図、設計施工標準といった専門的な業務資料に加え経験工学的に獲得された知識が多く存在するため、これらをドメイン分析モデルとして蓄積していくことは意義深い。保安制御ドメインの分析において特に重要なことは、ドメインエキスパートを交えてドメインに対するFTA／FMEA分析を行い、安全に関わる暗黙知を抽出し、形式知化してユーザ内に蓄積していくこと、及びユーザ、メーカー間で共有していくことであるが、今回の試行により、それをUMLドキュメントとして記述可能であることが確認できた。

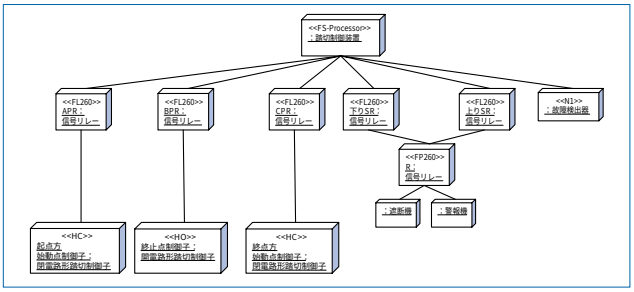


図４：ドメイン分析フェーズ段階での配置図

図５にドメイン分析フェーズのFTAを示す。

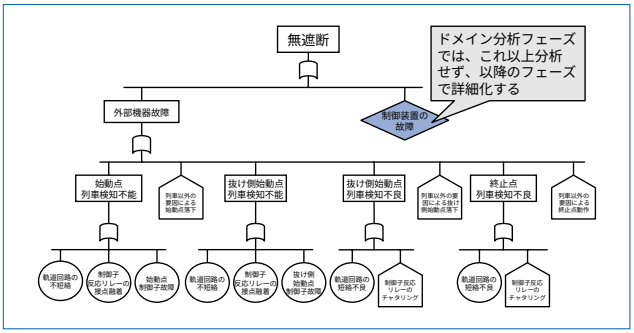


図５：ドメイン分析フェーズのFTA

このフェーズでの安全性解析の目的はドメインのハザードを特定し、それに結びつく要因を解析し安全性要求仕様を獲得することにある。本事例では、踏切のハザードは無遮断であり、無遮断に結びつく障害の分析を行った。FTA／FMEAはモノ中心に分析するという点でオブジェクト指向との親和性が高い。また、今回の試行において、共通のFT図をフェーズごとに詳細化していくことができることを確認した。これは、高度

な安全性を作りこんでいく上で非常に有効である。

(2) システム要求分析

開発対象となるシステムに必要な要求仕様の分析を行う。図6に、踏切の制御シーケンスの要求定義をシーケンス図で表記した事例を示す。

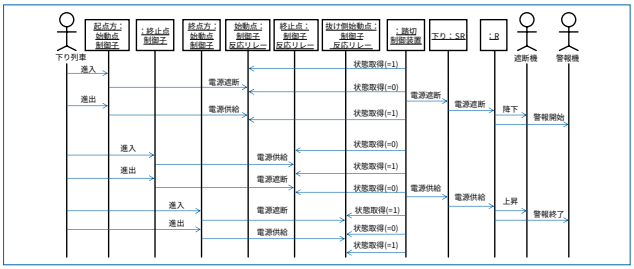


図6：踏切の制御シーケンス

(3) システム分析

開発対象システムを実現するためのハードウェア、及びソフトウェアアーキテクチャを決定する。このフェーズのFTA／FMEA分析では、すべての安全に関する要件を洗い出し、具体的な対策を検討する。

(4) ソフトウェア要求分析

開発対象となるソフトウェアに必要な要求仕様の分析を行い、機能仕様書を作成する。詳細なアルゴリズムは、このフェーズで定義される。図7に踏切制御子方式の単線踏切における下り列車の列車追跡アルゴリズムをステートチャート図で表記したものを示す

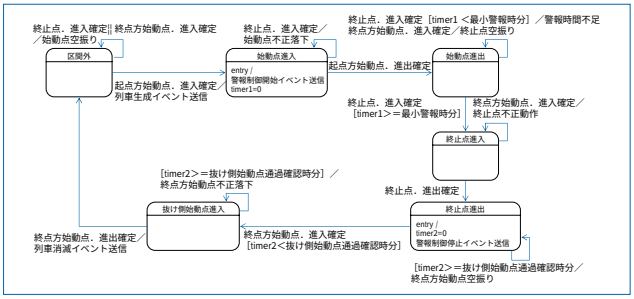


図7：列車追跡アルゴリズム

### 4.2 安全性規格との関係

保安制御用ソフトウェアの安全性規格として、IEC62279が制定されているが、現時点でオブジェクト指向開発の各個別手法について評価はされておらず今後整理を行っておく必要がある。以下に、開発の上流工程において、保安ソフトウェアの品質を確保する上で重要な点について示す。

(1) 開発プロセス

図3に今回試行した開発プロセスとIEC62279に例示された開発プロセスの対比を示しているが、オブジェクト指向開発だからといって開発プロセス、及び成果ドキュメントが大きく異なるということはない。

ただし、近年効率のよいオブジェクト指向開発プロセスとして提唱されている。スパイラル型や反復型の開発プロセスが保安ソフトウェア開発に適用できるかどうかについては、十分な検証が必要である。

(2) 安全性要求仕様の記述手法

保安装置の安全性要求仕様の記述においては、構造化手法、形式的仕様記述の採用が強く推奨されている。UMLは、形式的仕様記述手法に準ずる表記法を備えているが、それだけで十分なのかどうかは、さらなる検討を必要とする。

現時点での結論としては、保安制御ソフトウェア開発の上流工程においては、一般のソフトウェア開発と同様にそのメリットが十分に発揮される。しかしながら下流工程における課題の克服は未知数である。

## 5 おわりに

今回は、保安ソフトウェア開発の上流工程に対する、オブジェクト指向技術適用の試行を通して、その有効性を確認する研究を行った。主な成果として、以下の項目があげられる。

(1) オブジェクト指向技術にもとづく、保安ソフトウェアの開発プロセスの確立

(2) オブジェクト指向技術と安全性解析技術との統合

(3) UMLを活用したユーザ、メーカー間での知識共有手法の確立

なお、以下の点については課題として残っており、今後も検証を行っていく必要がある。

(1) 下流工程への適用

メーカー単独の作業工程であるが、成果物の評価手法を確立する必要がある。

(2) オブジェクト指向開発したソフトウェアの試験手法の確立

試験工程に対するオブジェクト指向技術については整理されていないため、今後検証方式を整理する必要がある。

(3) 規格を考慮した開発プロセスの運用方法の確立

ソフトウェアの安全性規格における、オブジェクト指向開発手法の位置づけを整理し、保安ソフトウェア開発プロセスの運用方法の確立が必要である。

**参考文献**

1) BERTRAND MEYER：オブジェクト指向入門, アスキー出版局, 1990.11.
2) 財団法人　鉄道総合技術研究所：列車保安制御システムの安全性技術指針, 1996.3.
3) 岸知二, 川口晃, 駒嵜克郎：ソフトウェアアーキテクチャにもとづく安全性ソフトウェアの開発, ソフトウェア工学112−7, 1996.1.