

平成 23 年度モデルベース開発技術部会活動報告書

独立行政法人情報処理推進機構
技術本部 ソフトウェア・エンジニアリング・センター
統合系システム・ソフトウェア信頼性基盤整備推進委員会

モデルベース開発技術部会

2013 年 1 月

目次

1.	はじめに	4
1.1.	背景と2011年度活動の概要	4
1.2.	実施内容	5
2.	統合システムモデリング技術 WG	6
2.1.	統合システムのモデリング	6
2.1.1.	統合システム開発の現状と課題	7
2.2.	2011年度検討事項(MDDとMBD)	7
2.2.1.	MDD	8
2.2.2.	MBD	9
2.2.3.	MDDとMBDの統合	10
2.2.4.	MDDとMBDの統合の意味	14
2.3.	統合システムモデリング技術WGの今後	15
2.3.1.	統合システムの課題を解決するために	15
2.4.	まとめ	17
3.	ユーザモデリング技術WG	18
3.1.	製品開発における利用者の位置づけの変化	18
3.1.1.	ユーザとは	19
3.1.2.	ユーザモデルとは	19
3.1.3.	ユーザモデルの階層	19
3.1.4.	ユーザモデルの利用形態の現状	20
3.1.5.	モデルベース開発におけるユーザモデルの位置づけ	20
3.2.	ユーザモデルの新しい利用形態の可能性	21
3.2.1.	設計段階のユーザモデルの利用形態	21
3.2.2.	開発検証時のユーザモデルの利用形態	22
3.3.	ユーザプロファイリングを基にしたユーザモデリング	23
3.3.1.	ユーザプロファイルからユーザモデルへのリンク	23
3.3.2.	ユーザモデルとユーザプロファイル	24
3.4.	ユーザプロファイルを基にしたユーザモデル作成プロセス案	25
3.4.1.	ユーザモデルの作成プロセス	25
3.4.2.	製品への要求定義	27
3.4.3.	ユーザコンテキスト定義	27
3.4.4.	ユーザ仕様	27
3.4.5.	ユーザ振舞い仕様	27
3.4.6.	ユーザモデル	28
3.5.	課題	28
4.	消費者機械安全標準化PT	29
4.1.	消費者機械の機能安全	29
4.1.1.	OMG提案のオントロジモデル	31

4.2.	2011年度の活動.....	32
4.2.1.	活動内容.....	32
4.3.	2012年度に向けた活動提案.....	34
4.4.	おわりに.....	35
5.	付録 部会・WG・PTの委員構成と実施内容.....	36
	付録1 モデルベース開発技術部会.....	36
	表 1-1 委員一覧(2012年3月末時点).....	36
	表 1-2 実施内容.....	36
	付録2 統合システムモデリング技術WG.....	36
	表 2-1 委員一覧(2012年3月末時点).....	36
	表 2-2 実施内容.....	37
	付録3 ユーザモデリング技術WG.....	37
	表 3-1 委員一覧(2012年3月末時点.....)	37
	表 3-2 実施内容.....	38
	付録4 消費者機械安全標準化PT.....	39
	表 4-1 委員一覧(2012年3月末時点).....	39
	表 4-2 実施内容.....	39

1. はじめに

1.1. 背景と2011年度活動の概要

(独)情報処理推進機構 技術本部 ソフトウェア・エンジニアリング・センター（以下、IPA/SECと略す）は、情報システムが組込み製品を含む様々なデバイス等と有機的に連携する一体的システム（統合システム）に変化しつつある状況を踏まえ、2009年度より「高信頼開発手法」及び利用者品質に着目した設計品質の向上技法の検討に着手しており、2010年度は「統合系システム・ソフトウェア信頼性基盤整備推進委員会 モデルベース開発技術部会」を設置し、更に検討を進めてきた。

2011年度は2010年度の検討結果を受けつつ、下記の3項目を重要事項と捉え、2つのWGと1つのPTにて討議検討を行った。

(1)「モデルベース開発技術」の適用領域の拡大（統合システムモデリング技術WGにて検討）

「障害波及性、システム安定性等今後増大する統合システムにおける主要リスク要因を設計段階で低減するために必要な技術を整理する」ことを目的として、「統合システムのリスクを低減するためのモデリング技術」について検討した。

具体的には、リスクを低減するモデリングとして、ソフトウェア開発で代表的なモデリング手法であるMDD¹とMBD²が挙げられるため、それらの適用性に関して検討を行った。

(2)「モデルベース開発技術」において未開拓な技術領域の確立（ユーザモデリング技術WGにて検討）

「多様なユーザ特性をモデル化するための標準的なプロセスを定義するとともに、現状把握のための利用者品質の確保に向けたユーザモデリング技術実用化調査を実施する」ことで、「ユーザ（人間系）のプロファイルを基にユーザモデルを作成するための手順の確立」について検討を行った。

(3)「消費者機械の機能安全」をOMGに提案（消費者機械安全標準化PTにて検討）

要求変化が速く利用形態が多様な消費者機械³の特性を踏まえたディペンダビリティを保証する枠組みを構築するため、2011年12月より、統合システムモデリング技術WGの直下に「消費者機械安全標準化PT」を設置して、OMG⁴に対して消費者機械の機能安全に関する標準を提案していくこととした。

具体的には、消費者機械の安全性、信頼性、セキュリティを含めたディペンダビリティを保証する枠組みについて検討を行い、標準化に向けてOMGに提案を行った結果、OMGよりRFI（Request for Information）が発行された。

本報告書は本部会の2011年度活動成果及び関連調査結果をとりまとめたものである。

¹ Model Driven Development の略で、主に情報系のモデルベース開発手法

² Model Base Development の略で、主に組込み系の狭義のモデルベース開発

³ 消費者機械は一般のユーザが利用する自動車、サービスロボット、家電、スマートハウスなどの機械製品に対する造語

⁴ Object Management Group の略で、標準化を推進している組織である

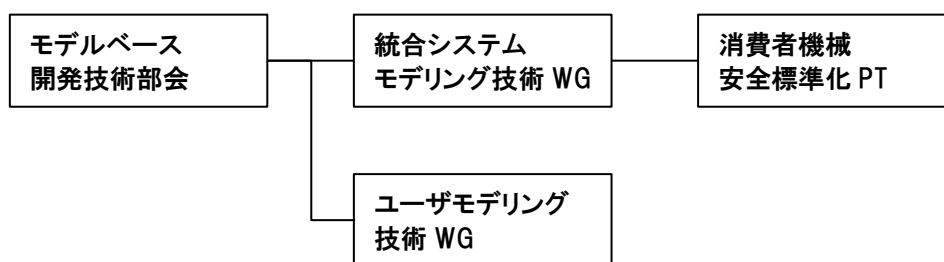


図 1-1 2011 年度モデルベース開発技術部会構成

1.2. 実施内容

第1回モデルベース開発技術部会を2011年10月に開催し、各WG活動に関する説明を行った。その後、各WGに活動の場を移し、2011年10月から2012年2月におよそ月1回ペースで3～5回開催した。WGの活動終了後の2011年3月に第2回部会を開催し、年度の活動報告と次年度の活動計画について報告を行った。

各部会・WG・PTの委員構成、及び開催時期、議題は付録に示す。

2. 統合システムモデリング技術 WG

統合システムモデリング技術 WG では、2011 年度の目的である「障害波及性、システム安定性等今後増大する統合システムにおける主要リスク要因を設計段階で低減するために必要な技術を整理する」のため、「統合システムのリスクを低減するためのモデリング技術」について討議検討を重ねた。

本章では 2011 年度の統合システムモデリング技術 WG の活動について報告する。

2.1. 統合システムのモデリング

そもそも統合システムとはどのようなものか、2010 年度のモデルベース開発技術部会の報告書で図 2-1 を掲載した。

統合システムは複数のシステムが関連して相互作用を行っている。ここで言うシステムとは情報システムや組込みシステムが含まれる。これらは目的や環境が違うために、開発のアプローチも大きく異なる。

なぜなら、情報システムは分散系（データの処理など）のみを扱うが、組込みシステムは物理現象などの連続系（メカ制御など）を扱うことが多い。扱っている系が違うシステム同士を繋ぐことで発生する問題も多い。

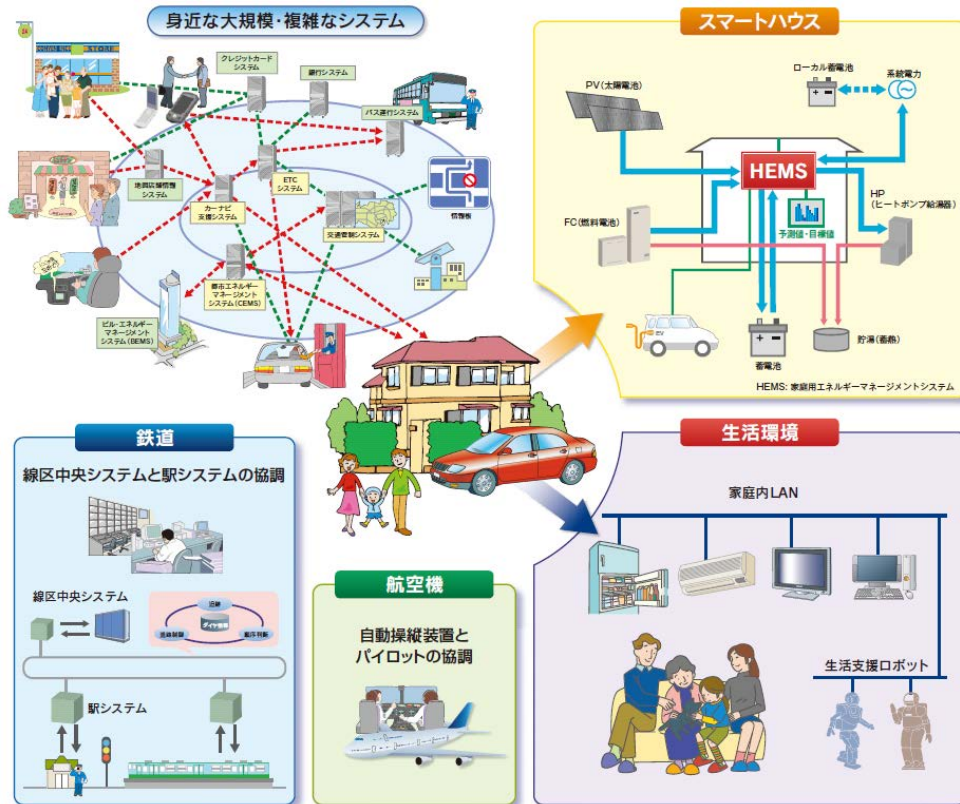


図 2-1 身近な統合システム

複雑化した上に系の違うシステム同士が連携するような統合システムでは、他のシステムを経由して繋がっている別のシステムのことは全く分からないことも多い。しかし、統合システムには目的があり、その目的を実現するために様々なシステムと連携をしている。必要に応じて中身の見えないブラックボックス化したシステムや全体が把握できないインフラを使うこともあるが、障害の波及は最小限に留めなければならないし、統合システムとして安定した動作を保証できなければならない。そこで、統合システムの信頼性向上のためには、統合システムを構成する情報システム（主に離散系）と組込みシステム（主に連続系）を包含し、システム全体の安全性、信頼性等を扱うことのできるようなモデル手法が必要とされる。

2.1.1. 統合システム開発の現状と課題

- 統合システム開発の現状
 - 統合システムの上流設計段階で、構成要素となる情報システムと組込システムのサブシステムに分割し、サブシステムごとに独立に開発
 - 情報システムと組込システムでは開発者も開発手法も異なる
 - 例) 情報システム：SI ベンダ、組込システム：装置メーカー
 - 構成要素の信頼性評価が実施されていても、全体システムとしての信頼性評価が不充情報システムと組込システムの統合は「組合せ型」であり、統合化がなされていないものが多い。
- 統合システムの課題
 - 組込みシステムの障害が情報システムに想定外の影響を与える危険性があり、他方情報システムの障害が組込みシステムに想定外の影響を与える危険性がある。
 - ⇒ 障害波及性、システム安定性、サービス継続性の面で潜在リスクが残存

※出典：「統合システム設計環境に関する調査研究」経産省 平成21年3月

http://www.meti.go.jp/policy/mono_info_service/joho/downloadfiles/2009software_research/01_togo.pdf

2.2. 2011 年度検討事項(MDD と MBD)

「統合システム全体のリスクを低減するためのモデリング」に対して、2011 年度の WG での討議は、情報システムのモデルベース開発の代表である MDD と組込みシステムのソフトウェアにおけるモデルベース開発の代表である MBD を、如何に統合システム全体に適用できるようにするかの検討を行った。

主に情報システム（離散系）の開発で使われているMDDはUMLを使用した開発が中心であり、主に組込みシステム（連続系）の開発で使われているMBDはMATLAB⁵ /Simulink⁶を使用し

⁵ Mathworks 社の製品で、数値解析ソフトウェアで使うプログラミング言語

⁶ Mathworks 社の製品で、マルチドメインシミュレーションシステム

た開発が中心となっている。この両者について比較検討を行うとともに、これらの手法を統合してそれぞれの弱点を補うことで、統合システム全体のリスクを低減すること（課題の解決）ができるのではという観点から、WGで討議した。

2.2.1. MDD

(1) MDD の概要

MDD はソフトウェア開発の上流工程から UML を使って抽象的なモデルを作成し、徐々に詳細化してコードへと落としていく。最近では自動コード生成やモデル検証なども可能なツールが用意されている。

このため MDD は、ソフトウェア開発の様々なリスクを低減することができる手法であり、組み込みシステムの開発でも注目を集めている。

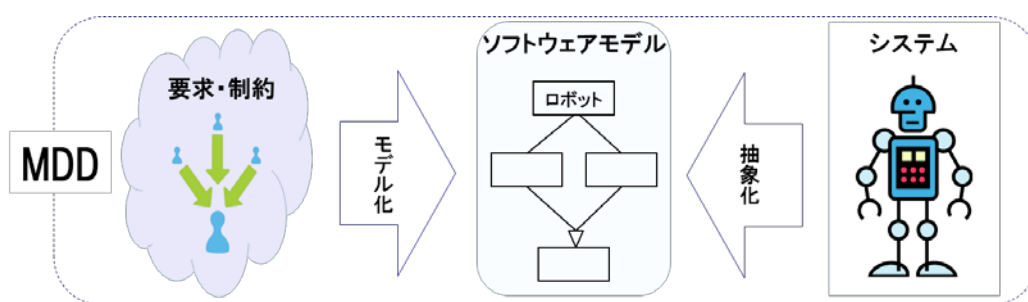


図 2-2 MDD によるモデル化

(2) MDD のモデル構成

- ・構造モデル
 - クラス図：クラス間の関係と各クラスのデータ要素の合意形成を図る
 - オブジェクト図：インスタンス間の関係を記述する
- ・振舞いモデル
 - ユースケース図：システムが提供するサービスとアクター（人または外部システム）の関係を記述する
 - 状態マシン図：トップレベルでは環境とのイベントのやり取りに、また構成要素では要素間のイベントのやり取りによる合意形成を図る
 - シーケンス図：シーケンシャルな振舞いを記述でき、振舞いの定義やシミュレーション結果を記述できる
 - コミュニケーション図：シーケンス図と同様にシーケンシャルな振舞いを記述できるが、インスタンス間の構成を中心に振舞いを記述する
 - アクティビティ図：通常はシナリオの記述に使用することが多いが、データフローに相当する記述も可能である

(3) MDD の弱点

MDD の制約としては、主に情報系システム（離散系）で使われており、制御対象モデル、制御ましい振舞いの定義から制御アルゴリズム（制御仕様）を導出できない、いわゆる連続系の記述方法を持たず、離散系のみしか扱うことができない。（例：エンジンの残留ガス推定ロジックを導出できない）

記述方法にもよるが、UML などの準形式手法では厳密性が失われる場合があり、形式手法では厳密に表現できるが、合意形成を図ることが困難になる。いずれにしても連続系は表現ができないので、連続系をどのように扱うかが論点になる。

したがって、MDD は統合システムにおけるソフトウェアのリスクを低減することはできるが、連続系を扱えないため統合システム全体のリスクを低減することは困難である。WG でも何度か指摘はあったが、ソフトウェアの枠を超えるまでには至らなかった。

2.2.2. MBD

(1) MBD の概要

MBD は (MATLAB®/Simulink®などで) 実現のためのモデルを作成して、シミュレーションなどを行いながらコードを自動生成する。

「広義の MBD」はモデルで開発をすること全般 (MDD や狭義の MBD が含まれる) を指し、特に MATLAB®/Simulink®を適用する場合に英語圏では、Model Based Development with MATLAB®/Simulink®と表現するのが一般的である。

一方、ここで扱っている MBD は日本固有の「狭義の MBD」であり、主に MATLAB®/Simulink®などを使って、(トップダウンに仕様から詳細化・具現化していくのではなく) 開発者が集まって日本的に「すり合わせ」を行いながら制御ソフトを開発することを指す。したがって、World Wide に通用する呼び名ではない。

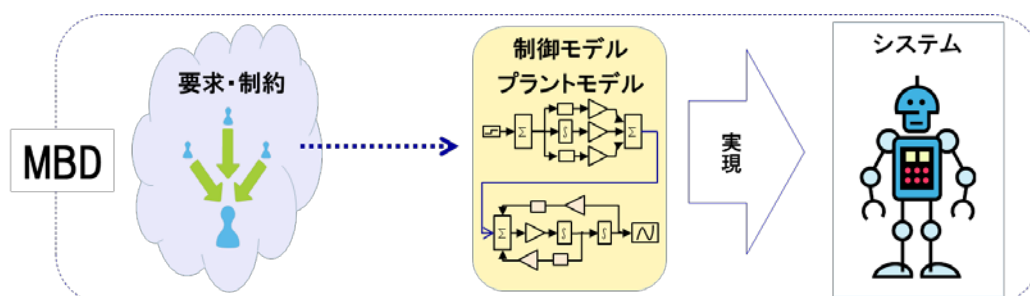


図 2-3 MBD によるモデル化

(2) MBD のモデル構成

- ・動的振舞いモデル

- Data Flow(DF)とControl Flow(CF)の混在系、離散事象系と連続事象系の混在系(ハイブリッドシステムモデル)を扱うことができ、DFはSimulink®/SimScape®⁷、CFはStateFlowが一般的であるが、これらに限定はされていない。
 なお、離散事象系は扱えるが、情報システム全体に適用するには、データベースやデータ構造が記述できないなどの点で記述能力が不足している。
- ホワイトボックスモデル(構造を明示的に持つ。例:物理モデル)、ブラックボックスモデル(構造を明示的に持たない。例:実験式)
- On line (Real time)モデル、Off line モデル
- データモデル
 - データ(メタデータ:プラント仕様、要求・制約、プロセス、検証データ、プラントモデル、制御装置モデル、コンフィグレーションデータ、履歴など)

(3) MBD の弱点

検証項目のリスト、制約と望ましい振舞いの定義の精度を上げることは、個人のスキルに依存する。(例:漏れや抜けが頻繁に発生。イテレーションの効率が人に依存する)

また実現のモデルが中心で、要求からのトレーサビリティが不明瞭である。

2.2.3. MDD と MBD の統合

またそれぞれの弱点を補うために、これらの手法を統合することで統合システムのリスクを低減すること(課題の解決)ができるのではという観点から、WG で討議されたその過程を報告する。

モデル名		MDD	MBD
構造モデル		○	—
分析モデル		○	コントロールフロー相当
シナリオモデル	ユースケース図	○	—
	シーケンス図	○	要求&シミュレーション結果
	コミュニケーション図	○	—
	アクティビティ図	○	データフロー相当
制御対象モデル		—	○
制御装置モデル		—	○

表 2-1 MDD と MBD のモデル比較

⁷ Mathwork 社の製品で、マルチドメインの制御対象モデルのベースになる

表 2-1 は、MDD で扱えるモデルと MBD で扱えるモデルを比較している。表でも明らかなおお、MDD と MBD はシステムのモデルを補完するような位置づけとも考えられるため、まずモデルを統合することで、2つの手法を統合することを検討する。

(1) MDD と MBD の違い

- ・ MDD : 状態遷移よりスタートする (データフローからスタートする場合もある)

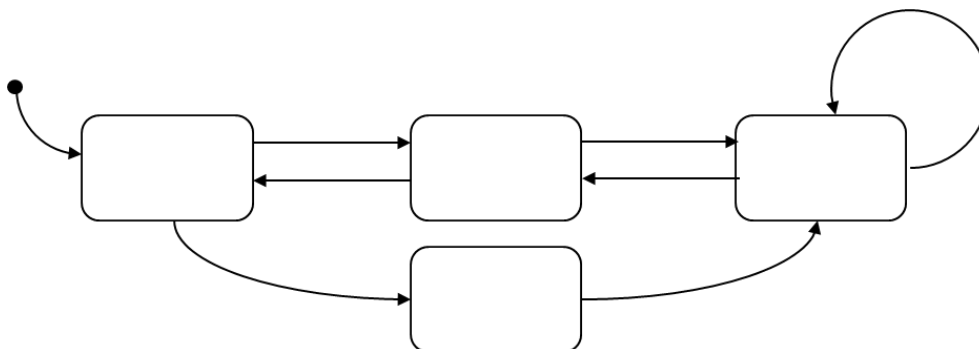


図 2-4 MDD の状態マシン図

- ・ MBD : データフロー線図よりスタート

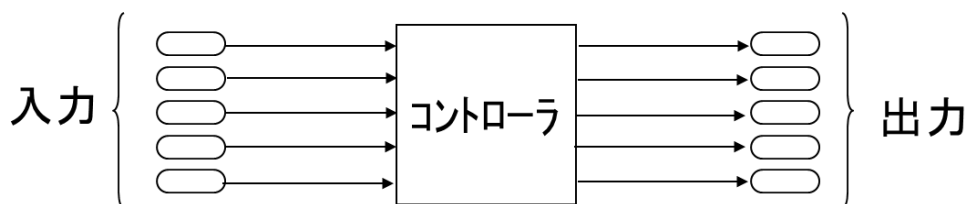


図 2-5 MBD のデータフロー線図

状態遷移図 (State Chart+Flow) からのスタートは可能だが、データフローがトッププレイヤーになるのが普通。全ての入出力を記述する。(RPCなどで実際に繋ぐことが前提)

- ・ MDD : データフローと状態遷移の混在する記述は行えない
- ・ MBD : 状態遷移図 (コントロールフローと解釈。State Chart+Flow Chart) とデータフロー線図を両方とも記述できる

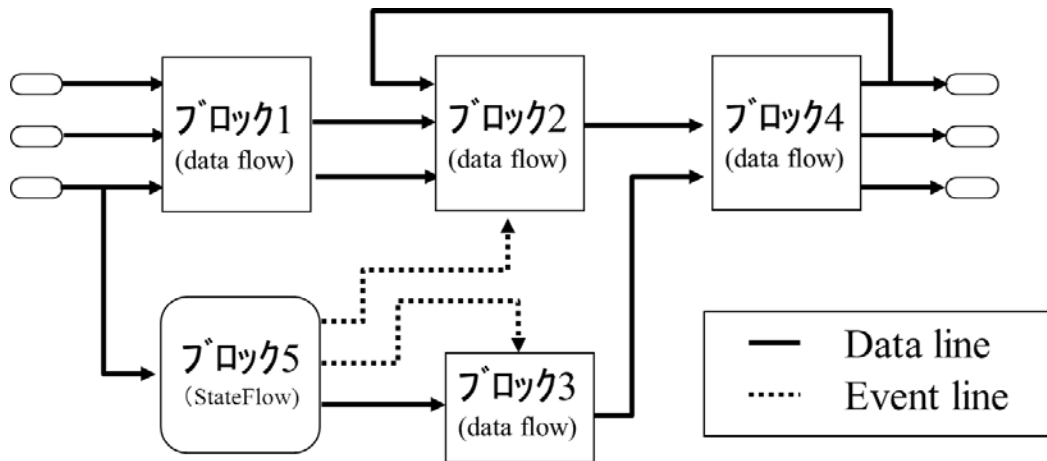


図 2-6 MBD の混在記述

- MDD : 要求文書からスタート (要求文書をインプット)
- MBD : ラフな要求からスタート (Agile 的) (要求文書は初期条件かアウトプット)
 - 必ずしも要求文書はインプットとしては必要ない要求文書は開発過程でできあがる

- MDD : アーキテクチャ中心の開発

アーキテクチャ中心とはソフトウェアを動かすコア・アーキテクチャをできるだけ早い段階で確立させるアプローチである。開発の全ての作業においてこのアーキテクチャを常に意識することを重要である。

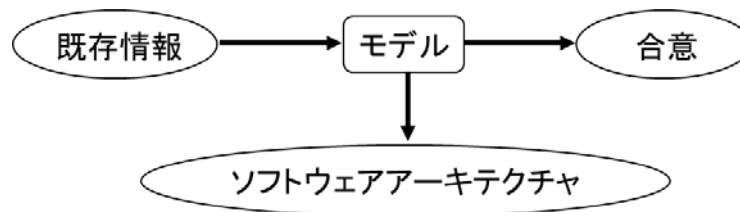


図 2-7 アーキテクチャ中心のアプローチ

- MBD : すり合わせによる開発

日本の従来の組み込み開発はすり合わせ型の開発である。すり合わせ型開発の対極は組み合わせ型開発で、すり合わせ型とは試行錯誤や調整を積み上げていく開発方法である。

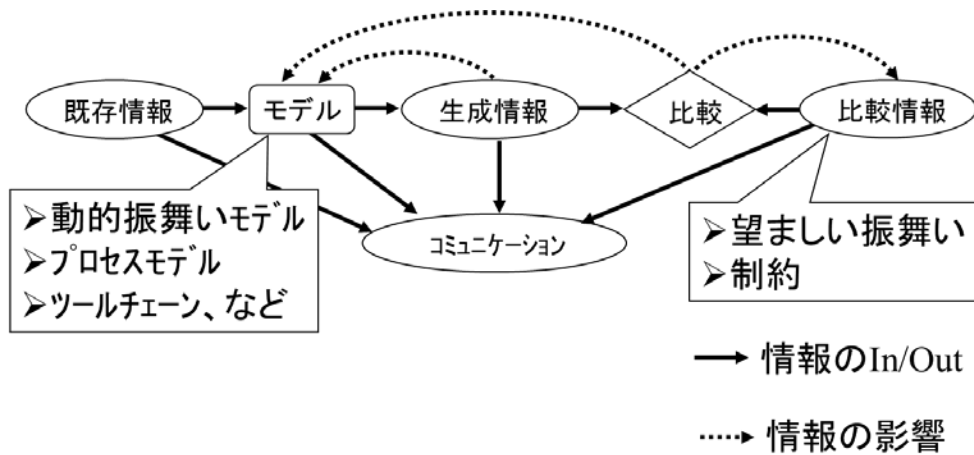


図 2-8 MBD のすり合わせ開発

(2) MDD と MBD の統合のイメージ

MDD と MBD の関係は、従来はそれぞれ別の手法として独立しているため、MBD と MDD が組み合わせて使われることはほとんどなかった。

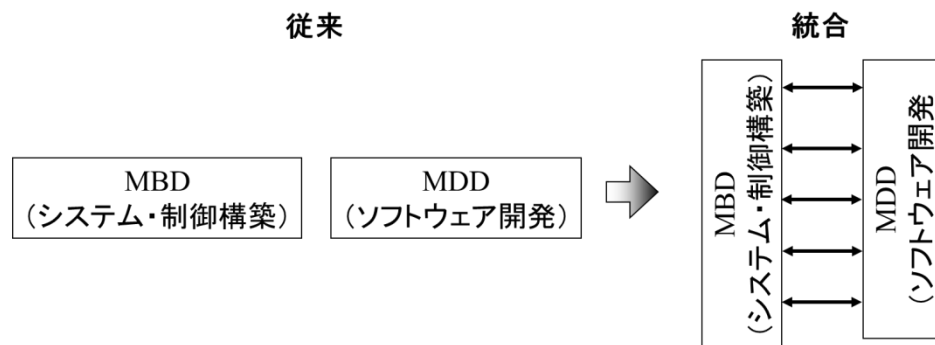


図 2-9 MDD と MBD の統合

図 2-9 の統合のイメージは互いに MDD と MBD が相互に利用し合うようなイメージに見えるが、互いの良いところを取り入れると考える方がより現実的と考えられる。表 2-2 のようにモデルをまず統合して、互いの欠落を埋めるように補うことも 1 つの方法と考えられるが、実用に耐えられるかどうかは今後の検討が必要である。

実際には上流工程では要求からアプローチできる MDD を、下流工程では実現を前提とした MBD を適用することが現実的と考える。

モデル名		統合
構造モデル		MDD
分析モデル		MDD+MBD
シナリオモデル	ユースケース図	MDD
	シーケンス図	MDD+MBD
	コミュニケーション図	MDD+MBD
	アクティビティ図	MDD+MBD
制御対象モデル		MBD
制御装置モデル		MBD

表 2-2 MDD と MBD のモデルの統合

WG では表 2-1 を基にして検討を行い、表 2-2 のようなモデルの統合に関する結論を得た。具体的にどのようにモデルを統合すべきかは、今後更にツール要件などを考慮しながら検討する必要がある。

(3) MDD と MBD の統合に向けた課題

- (a) 統合システムを効率よく開発する方法論、ツールの要件を整備する
- (b) 統合システムの開發生産性向上、メンテナンス、サービスの効率的手法を整備する
- (c) モデリングプロセスの明確化と共有化を行う
- (d) モデル対象とモデルの分類とその関係を定義する

2.2.4. MDD と MBD の統合の意味

「統合システム全体のリスクを低減するためのモデリング」に対して、MDD と MBD の統合との観点での検討により、ソフトウェアにおける解決策はある程度の方向性を見出すことができた。また、この検討を通して、MDD 経験者と MBD 経験者がお互いの手法の違いや弱点を理解することもできた。

しかし、「MDD と MBD の統合に向けた課題」でも明らかのように、「統合システムを効率よく開発を進めする方法論」は、統合システム全体を見渡すことができるモデルが必要で、そのシステム間の関係も明確にできなければならない。「統合システムの開發生産性向上、メンテナンス、サービスの効率的手法」は、ソフトウェアだけで解決できない要素を含んでいる。

つまり、「ソフトウェア」ではなく「システム」という観点で検討する必要がある。つまり「ソフトウェアエンジニアリング」だけでなく、「システムズエンジニアリング」を検討する必要があると考える。

2.3. 統合システムモデリング技術 WG の今後

2.3.1. 統合システムの課題を解決するために

個々のシステムを組み合わせて統合システムを作るという発想では課題を解決することは難しい。統合システムとしての目的や要求・構造・振舞いを明らかにして、個々のシステムに分割 (decompose) する必要がある。こうすることで、全体としての統合システムの信頼性評価を得ることができる。

これはソフトウェアだけで解決できる問題ではなく、統合システム全体 (System of Systems) を扱うことができなければ難しいと考える。そこでシステムズエンジニアリングによる解決を検討する必要がある。

モデルを活用したシステムズエンジニアリングである MBSE は特に統合システムの課題を解決するために必要な要素を多く持ち合わせている。MBSE はそもそも MDD の要素を多く含んでいて、MDD をシステムに拡張した手法といっても過言ではない。したがって、MBSE を検討することで、システムは MDD を拡張した MBSE で、ソフトウェアは MDD+MBD という組合せも可能になる。ここで MBSE について簡単に説明する。

図 2-10 は MBSE の基本的なモデル間の構造を表しているが、まずシステムを適切 (QCDSE⁸のバランスを考慮して) にハードウェア (Hardware Models) とソフトウェア (Software Models) に分割 (decompose) することができることを意味している。また、制約などが厳しいものはフイージビリティなども含めてモデル (Analysis Models) を使って分析することができる。さらに検証のためのモデル (Verification Models) により、モデルを使用した信頼性評価を扱うことができるようになる。

⁸ 通常の QCD (Quality, Cost, Delivery) に加えて SE (Safety, Environment) が製品における重視すべき要素である

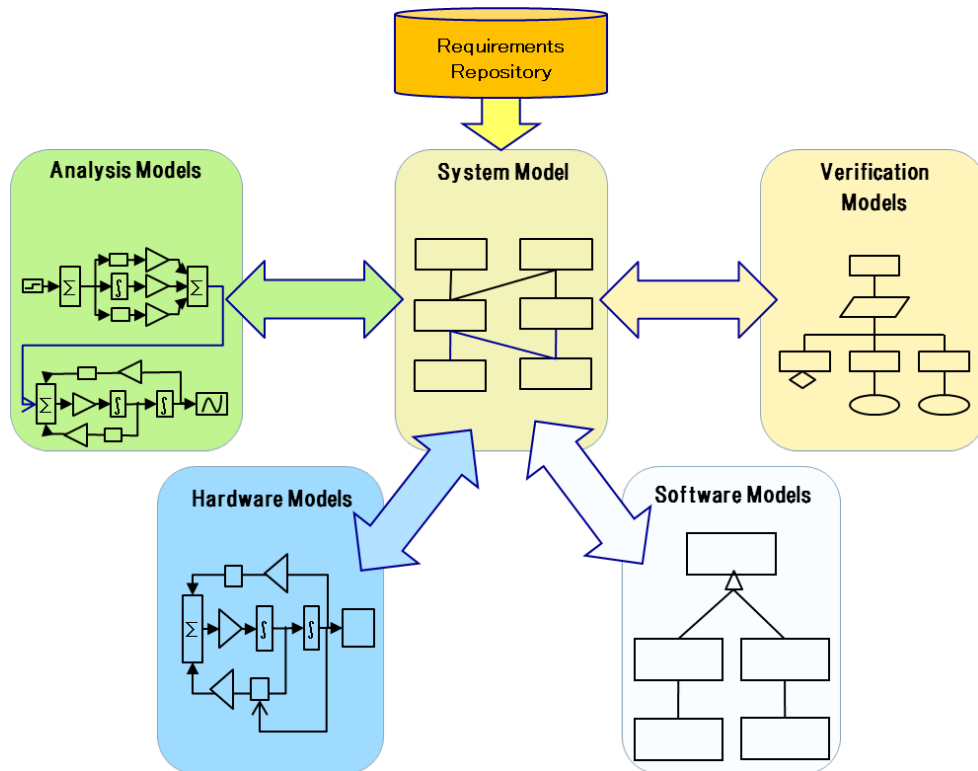


図 2-10 MBSE の基本構造

さらに、MBSE はシステムの階層構造を扱うことができるために、System of Systems Level から Element Level (Component を含む) まで扱うことができる。

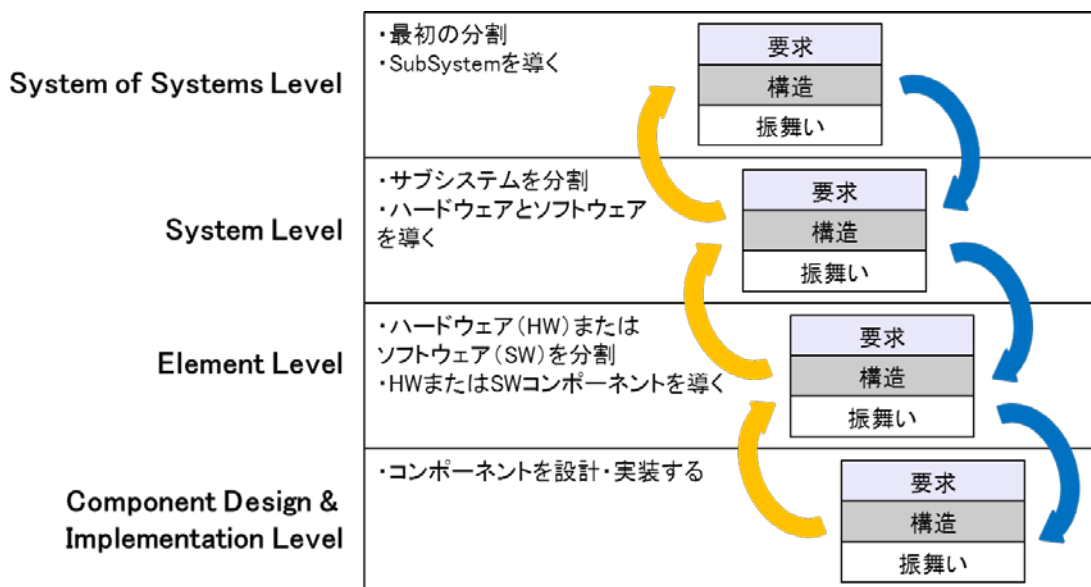


図 2-11 MBSE のシステムの階層化

この階層構造により、System of Systems Level から Element Level (Component を含む) まで信頼性評価のトレーサビリティを確保することができる。

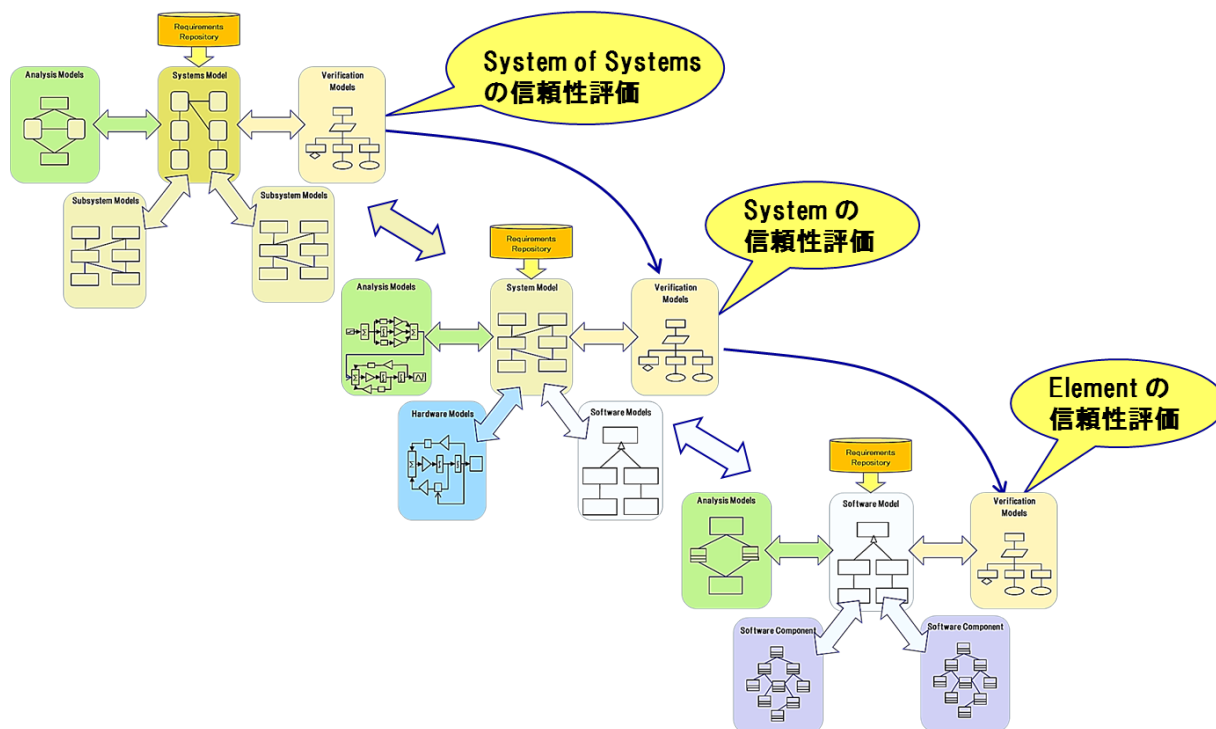


図 2-12 MBSE による信頼性評価のトレーサビリティ

2.4. まとめ

2011 年度は「組込みシステムの障害が情報システムに想定外の影響を与える危険性があり、他方情報システムの障害が組込みシステムに想定外の影響を与える危険性がある」という統合システムの課題に対して、MDD と MBD の統合ということを検討し、有効である可能性を見出した。

しかし、MDD と MBD の統合だけでは、統合システムにおけるソフトウェアの課題解決には有効と思われるが、統合システム全体の課題解決は難しいことも分かってきた。これを受けて 2012 年度はシステムズエンジニアリング、特にモデルベースのシステムズエンジニアリングである MBSE を検討して、2011 年度で検討した MDD と MBD の統合へと繋げていく予定である。

3. ユーザモデリング技術 WG

製品に対する満足度の指針の 1 つである「利用時の品質」の向上のためには、製品に対するユーザの振舞いを理解した上で製品を設計・開発する必要がある。ユーザの振舞いを定義するユーザモデルは設計検証や開発検証だけでなく、製品設計時においても重要になると考えられる。ユーザモデリング技術 WG ではユーザモデルのモデル化技術の要件をまとめるため、ユーザモデルを構築する技術に関する調査を行うとともに、ユーザプロフィールからユーザモデルを構築するまでの開発プロセスについて検討を行った。本章では 2011 年度のユーザモデリング技術 WG の活動について報告する。

3.1. 製品開発における利用者の位置づけの変化

利用者が多様化し、製品に対する満足度の指針の 1 つである「利用時品質」に関する基準も多元化しており、製品設計や検証が困難になってきている。特に、幼児や高齢者、身体障害者にとっての製品の利用時品質を理解し、確保することは難しい。

これまで、日本製品は利用時品質よりも絶対的製品品質を武器に製品開発を行ってきた。しかし、利用者の多様化によって、平均的な顧客像に対する絶対的製品品質だけでは多様化した利用者の満足が得られない状況となった。

また、日本製品の世界戦略も、他国の製品と比較した絶対的製品品質を武器にしてきた。しかし、他国の製品品質の向上に伴い、製品品質の差が縮小してきたため、日本製品の国際競争力が低下している。

そこで、製品品質の差別化のために仕向地⁹の利用者にとっての「利用時品質」の向上を目指して、仕向地用の製品を仕向地で開発するようになってきたが、それが原因で日本の産業の空洞化が進行している。

国内、国外ともに重要となっている「利用時品質」の向上を、利用者を直接知る機会の少ない開発者だけで対応することは困難である。利用者を意識した設計と検証を実現するために「利用者像」を明確化し、製品開発の全ライフサイクルで継承し、共有化することが必要になってきている。

本節では、まず WG の議論の前提となる利用者（ユーザモデル）の状況について概説する。

⁹ ここでは製品が出荷され消費される日本国外の場所のこと。文化等の違いにより日本とは異なる使い方をされることもあるので製品開発時考慮する必要がある。

3.1.1. ユーザとは

商品の企画段階では、マーケティングの観点で「顧客（カスタマ）」をプロファイリングしてきた。しかし、この段階では「顧客」を「購入者」の側面だけでとらえることが多く、製品開発の現場まで「顧客」像を継承して共有し、利用する考え方は少なかった。

本報告書における「ユーザ」は、製品の「利用者」を意味し、製品に対して直接接して操作する役割を持つ者を指す。「ユーザ」は、購入者と同一である場合もあるが、役割として異なるため、「購入者＝ユーザ」の場合であったとしても、「利用者」の側面だけを抽出した「顧客」を意味する。

3.1.2. ユーザモデルとは

本報告書における「ユーザモデル」は、製品・サービスのユーザを代表する「アバター（化身）」であり、製品に対するユーザの振舞いを再現することのできるモデルを意味する。「モデル」には「典型」などの意味があり、ユーザモデルは「典型的利用者の表現」の意味で使う。広義ではユーザプロファイルもユーザモデルと考えられるが、本報告書においては「振舞い」を定義するものをユーザモデルと呼ぶ。

3.1.3. ユーザモデルの階層

ユーザモデルは新しい概念ではない。モデルベース開発において既に利用されている考え方である。特に、自動車産業では「ドライバモデル」という名称で、1970年代から利用されている。

当年度実施した「利用者品質の確保に向けたユーザモデリング技術実用化調査」（以下、「ユーザモデリング調査」と略す）において、Michon は、代表的なユーザモデルであるドライバモデルのタスクに関して階層の考え方を導入し、生活習慣に関わる「振舞いレベル」、基本計画に関わる「戦略レベル」、意識行動に関わる「戦術レベル」、無意識行動に関わる「操作レベル」の4階層に分類していることが分かった。

Michon の「振舞いレベル」は本報告書の「振舞い」とは意味が異なるので本報告書を読む場合には注意が必要である。Michon の「振舞いレベル」は「日常生活におけるドライバの一般的な振舞いを規定する態度、信条等」であり、一般的な行動様式のレベルである。「戦略レベル」は「運転の計画、目的地、休憩地」などの基本計画であり、「戦術レベル」は「目的地に着くために、いつ曲がる、早く到着するために車を追い越すプロセス」などの意識行動を対象としている。そして、最下層の「操作レベル」は、ハンドル、ブレーキ、アクセルなどによる車両の操作自体のレベルであり、「スピードの制御」、「カーブのすり抜け」、「レーンの維持」などの無意識行動を対象としている。

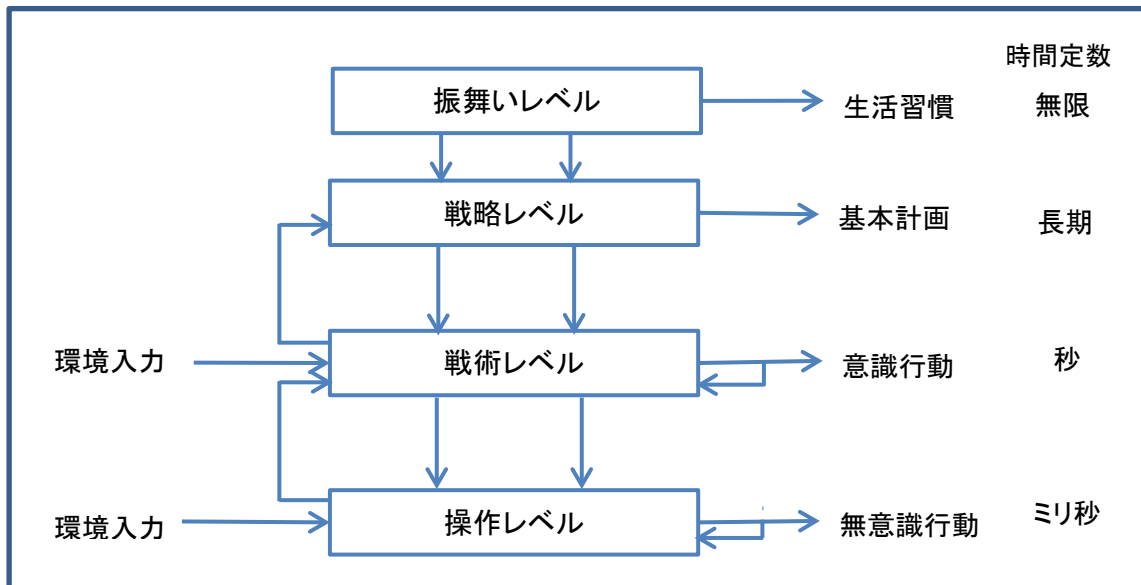


図 3-1 Michon によるタスク階層

3.1.4. ユーザモデルの利用形態の現状

モデルベース開発においてこれまで、ユーザモデルはモデルベース開発ツールや「MILS(Model In the Loop Simulator)」や「HILS(Hardware In the Loop Simulator)」の「検証」のシナリオの中で、代表的なユーザを再現するために利用されてきた。MILS はハードウェアを開発する前の段階で、設計の問題点の有無を確認するための設計検証を行うツールであり、HILS は開発したハードウェアの問題点の有無を確認するための開発検証を行うツールである。MILS や HILS では、「ユーザモデル」はシナリオの中で「特定の環境における代表的な操作」として表現されており、「ユーザモデル」を独立した形態で利用してはいない。

シナリオの中で使われるユーザモデルは、たとえば「特定の路面でのブレーキングにおけるブレーキ踏量」として表現される。

3.1.5. モデルベース開発におけるユーザモデルの位置づけ

ユーザモデルの代表であるドライバモデルは、「標準的運転者」をモデル化し、「製品」、「環境」と密接に関連させ、「すり合わせ」をしてシナリオに埋め込む形態で利用されてきた。この「すり合わせ」による手法は、ユーザモデルの振舞いとしての完成度は高いが、手間がかかるため、多様化するユーザに対応させるための柔軟性に欠けている。

また、ドライバモデルの利用形態としては検証が一般的であり、設計段階での利用は重要視されてこなかった。今後、多様化するユーザに対応させるためには、ユーザを「ユーザモデル」として独立して定義し、「製品」や「環境」、「シナリオ」と組み合わせて利用する形態が必要となる。

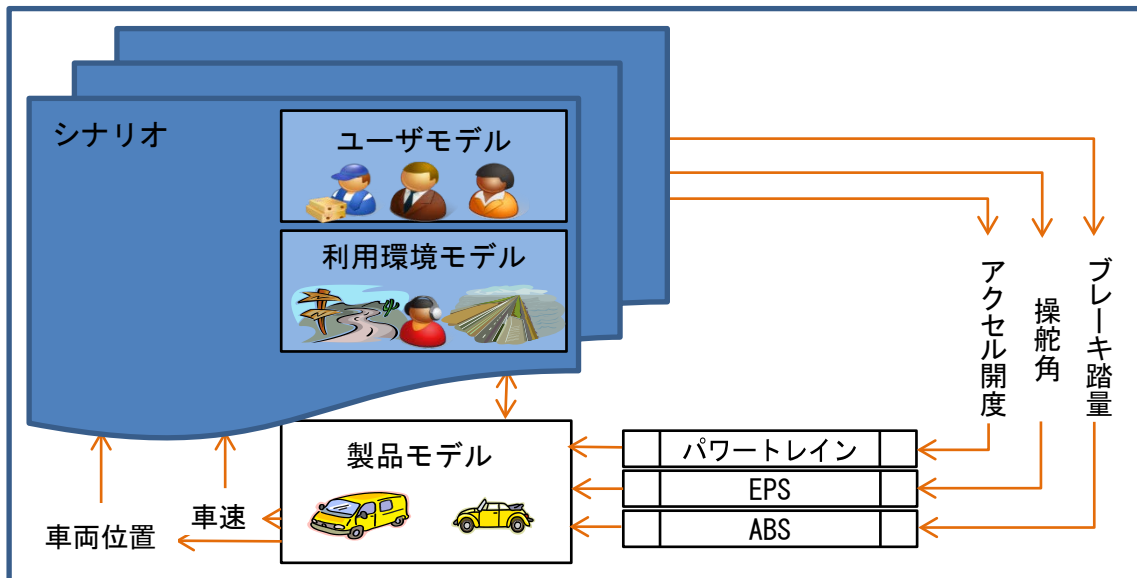


図 3-2 シナリオに埋め込まれたユーザモデル

3.2. ユーザモデルの新しい利用形態の可能性

製品企画の段階で製品の対象となる代表的な利用者が設定される。国内の利用者も多様化してきているが、製品の国際化に伴いその利用形態は増々多様化しており、それぞれの利用者に対しての利用時品質の向上が必要となっている。

国内、国外ともに重要となっている「利用時品質」の向上のためには、それぞれの利用者を理解し、製品を設計し、開発する必要がある。そのため、ユーザモデルは設計検証や開発検証だけでなく、今後、製品設計時においても更に重要になると考えられる。

ここでは、WG 内で共通的に認識されたユーザモデルの新しい利用形態（設計・開発時の利用）とその効果について説明する。

3.2.1. 設計段階のユーザモデルの利用形態

(1) 設計時のユーザモデルの利用形態

利用時品質を向上させるために重要な開発プロセスの最初の工程は、設計である。設計時に製品や利用環境だけではなく、利用者の特徴を把握できれば、利用者が必要としている利用時品質を製品設計に取り込むことができ、利用者が多様化したとしても必要とされる利用時品質の向上に反映できる。

しかし、利用者の特徴を単にリストアップするだけでは利用者像を設計から開発まで継承し、共有することは難しい。利用者像の継承や共有にはモデル化が有用である。

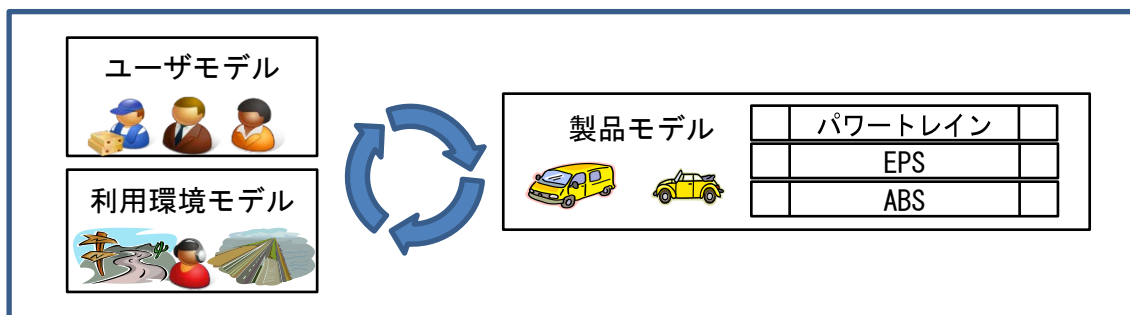


図 3-3 設計時におけるユーザモデル

(2) 設計検証時のユーザモデルの利用形態

設計時に想定した利用時品質が真に利用者の求める利用時品質であることを検証できれば、ハードウェアの試作を繰り返す必要がなくなる。そこで、利用者の代わりにユーザをモデル化した「ユーザモデル」に製品のモデルである制御モデルとプラントモデルを利用環境モデルに対応したシナリオで操作させることができれば利用時品質の検証が可能となる。

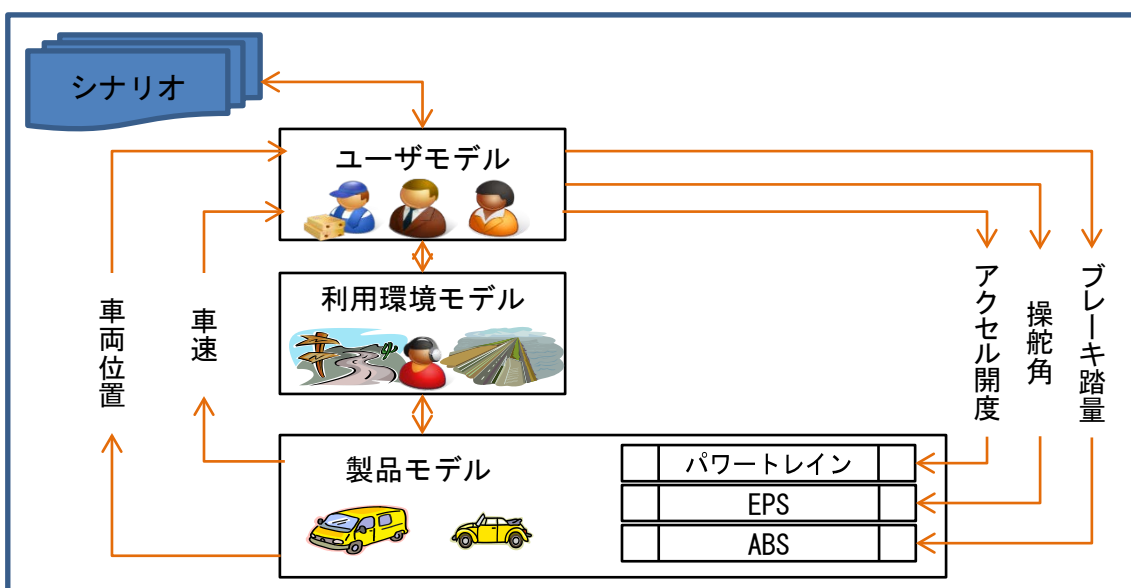


図 3-4 設計検証におけるユーザモデル

3.2.2. 開発検証時のユーザモデルの利用形態

設計時に作成したユーザモデルは、開発検証時においても利用可能である。ハードウェアの一部、または、全部が完成した時点で、実際にユーザに製品を利用させるように、ユーザモデルを利用環境モデルに対応したシナリオで操作させ、設計時の利用時品質の検証が可能となる。

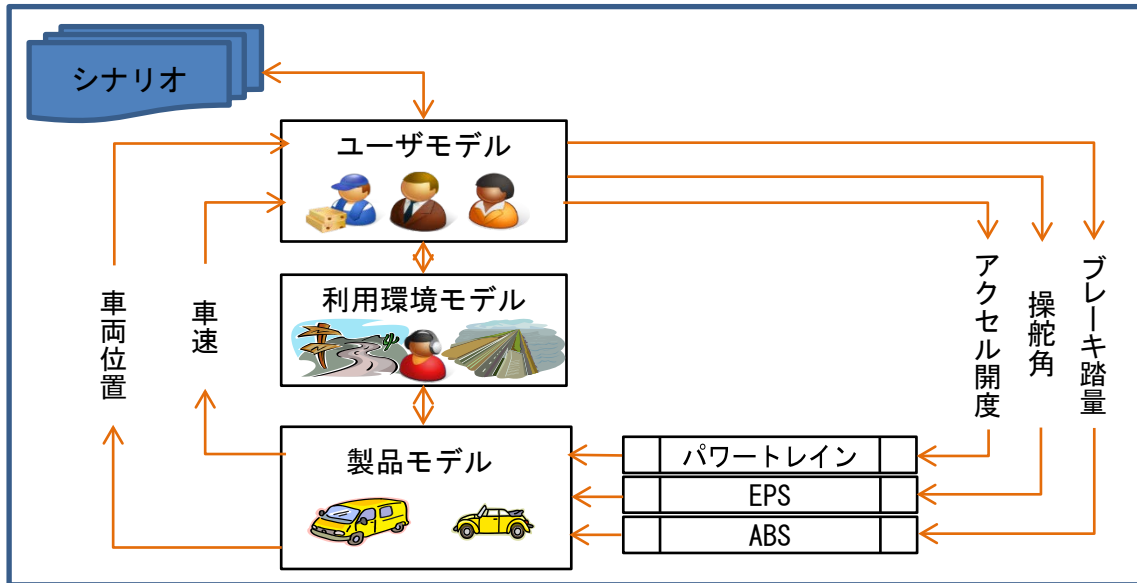


図 3-5 開発検証におけるユーザモデル

3.3. ユーザプロファイリングを基にしたユーザモデリング

製品企画時に製品顧客を調査し、利用者側面からユーザプロファイルを作成できれば、対象ユーザが必要とする利用時品質を設計し、実現し、検証できるようになる。つまり、ユーザプロファイルを基にユーザモデルを定義し、利用するプロセスを確立できれば、多様化するユーザにも対応した利用時品質を実現でき、利用者にとっても日本の産業にとっても有用と考えられる。

3.3.1. ユーザプロファイルからユーザモデルへのリンク

企画段階で調査した製品顧客のプロファイルは「購入者」の側面が多く、利用者としての側面を詳細に記述することは少なかった。そのため、製品顧客のプロファイルが企画段階以降に継承されず、共有されることはなかった。

しかし、顧客プロファイルに記載された特徴から利用時の振舞いを想定するための特徴を示すキーワードを取得できる。また、必要とされる利用時品質を実現することを前提に製品の顧客情報を収集し、ユーザプロファイルを作成することになれば、利用者としての側面を明確にし、利用時の振舞いに関わるキーワードを詳細に獲得できるようになる。

そこで、ユーザモデリング技術 WG では、「ユーザモデリング調査」の結果を参考に、製品企画時の製品顧客の利用者側面のプロファイルである「ユーザプロファイル」を基に「ユーザモデル」を作成し、製品モデルの構成要素である制御モデルとプラントモデルとともに、シナリオからの独立性を保ちながら、設計や設計検証、開発検証に利用する形態の実現性を検討した。

なお、上記の「ユーザモデリング調査」では、

- ①ユーザプロファイル手法・技術に関する調査
- ②モデルベース開発手法・技術におけるユーザモデルの取込みに関する調査

③ユーザプロフィールからユーザモデルを構築する手法・技術及びユーザデータに関する調査の3点に関して調査を実施している。

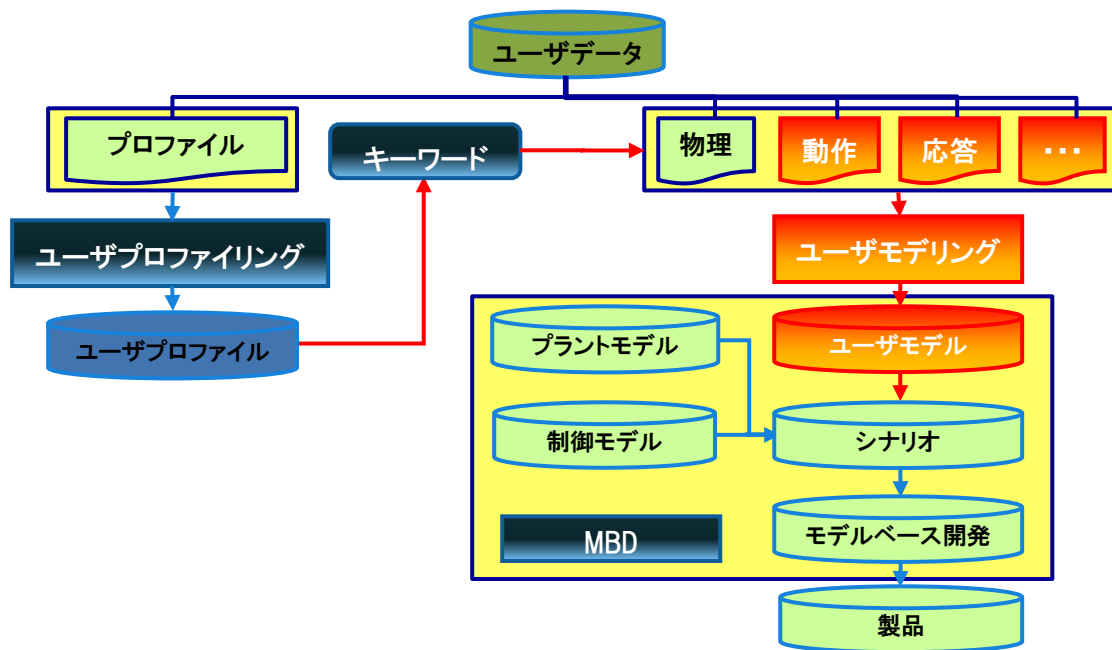


図 3-6 ユーザプロフィールを基にしたユーザモデルの全体の流れ

3.3.2. ユーザモデルとユーザプロフィール

「ユーザモデリング調査①」より、長年、ユーザモデルが各種研究されていることが分かった。たとえば、ドライバモデルに関しては 1970 年代から、Michon による「ドライバモデルの分類」や「ドライバのタスク階層」、Rasmussen による「3 次元ドライバモデル」と「循環運転プロセス」などの基本的研究がされてきた。また、Windsor 大学（カナダ）などでは人間の神経組織の信号伝達処理を模した「ニューラルネットワークを利用したドライバモデル」などの研究も行われている。しかし、ユーザプロフィールから直接ユーザモデルを作成する手法は存在していない。

類似した手法としては、EU の FP7 プロジェクトである VERITAS がある。VERITAS では身体的障害や認知障害をオントロジで記述した「抽象モデル」、特定の障害を持つユーザを表す「汎用的仮想ユーザモデル」、カスタマイズした「仮想ユーザモデル」などの研究もなされているが、高齢者や身障者以外を対象としていない。

更に「ユーザモデリング調査②」により、モデルベース開発にユーザモデルを適用することにより、より適用性の高い製品開発に繋げることのできる可能性についても確認することができた。

本ユーザモデリング技術 WG では、「ユーザモデリング調査③」を参考に、「ユーザプロフィール」を基に「ユーザモデル」を作成する手法を検討した。その結果、「ユーザプロフィール」から「ユーザモデル」を作成する際に、「製品への要求定義」、「ユーザコンテキスト定義」、「ユーザ仕様」、「ユーザ振舞い仕様」が必要であることが分かった。

また、「ユーザの振舞い仕様」はユーザプロファイルのキーワードと密接に関係しており、キーワードをインデックスとしたデータベースから「値・式」を抽出してユーザ仕様を定義する必要がある。「ユーザの振舞い仕様」としては「物理的寸法」、「動作」、「応答速度」などが必要となると考えられるが、現在、ユーザモデルを作成する際に有用なデータベースとしては「物理的寸法」が存在しているだけであることも、同調査で判明した。

3.4. ユーザプロファイルを基にしたユーザモデル作成プロセス案

製品企画時の顧客プロファイルに利用者の側面としての情報を追加することができれば、ユーザプロファイルを基にユーザモデルを作成するために必要な情報源となる。利用者の側面としての情報としては、「利用者が対象とする製品をどのような利用環境でどのように利用するか」という情報である。

次に、顧客の利用者の側面を基にしたユーザプロファイルからユーザモデルを作成し、製品や利用環境と組み合わせてユースケース図やシーケンス図を作成する。たとえば、「人の飛び出し時にも轢かない自動車運転」などのタスクを設定し、設計において利用時品質の向上をすることができる。

そして、ユーザモデルとタスクごとのユースケース図やシーケンス図を基に、モデルベース開発ツールを使い、ユーザモデルを入れ替えることのできるシナリオを作成することが可能となる。もちろん、このプロセスは一方通行ではなく、フィードバックで後戻りをしながら、ユーザモデルの完成に近づくことになる。

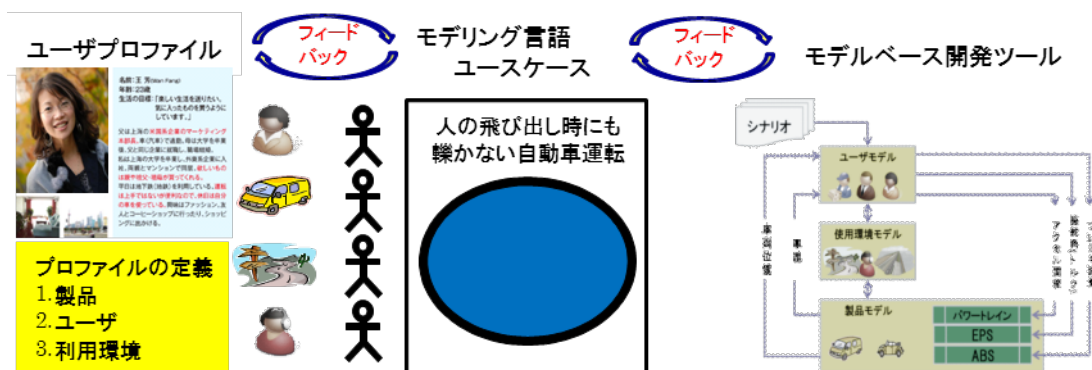


図 3-7 ユーザプロファイルからユーザモデルを作成し、ツールで利用するまでのプロセス
本図中ユーザプロファイルの写真・内容については架空のものであり、実在の人物とは関係ありません。

3.4.1. ユーザモデルの作成プロセス

製品開発においてモデルベース開発が普及し始めている。モデルベース開発といっても、「SysML」などの言語を使って設計を行う形態のものと、モデルベース開発ツールや「MILS(Model In the Loop Simulator)」や「HILS(Hardware In the Loop Simulator)」で開発から検証までを行う形態のものがある。現在、ユーザモデルを実現する手法としては開発から検証までを行う手法に偏っており、上流である要求定義や設計を網羅した手法は調査において見つかっていない。

本ユーザモデリング技術WGでは、顧客の利用者側面から作成したユーザプロフィールを基にしたユーザモデルの作成プロセスを、「ユーザプロフィール」、「製品への要求定義」、「ユーザコンテキスト定義」、「ユーザ仕様」、「ユーザ振舞い仕様」、モデルベース開発ツールで動作する「ユーザモデル」、の6段階で行うプロセスとして検討した。

- (1) 顧客の利用者側面を調査し、「ユーザプロフィール」を作成する。ユーザプロフィールは、Michonの「振舞いレベル」であり、「生活習慣」を表す。
- (2) 対象ユーザのプロフィールの利用環境を確認し、必要とされる利用時品質を明確にし、「製品への要求定義」を作成する。「製品への要求定義」の「利用時品質」の確認において、Michonの「戦略レベル」の「基本計画」を設定する。
- (3) ユーザプロフィールと製品への要求定義や設計仕様を基に「ユーザコンテキスト定義」を作成する。「ユーザコンテキスト定義」はMichonの「戦術レベル」であり、「意識行動」を表す。ここで、「ユーザ」を「製品」、「利用環境」、そして、利用の「シナリオ」から明確に分離する。
- (4) ユーザコンテキスト定義と、ユーザコンテキスト定義に基づいてユーザプロフィールから取り出したキーワード、キーワードをインデックスとしてデータベースから抽出したデータを基に「ユーザ仕様」を作成する。「ユーザ定義」はMichonの「操作レベル」であり、「無意識行動」を表す。
- (5) 「ユーザコンテキスト定義」と「ユーザ仕様」を基に「ユーザ振舞い仕様」を作成する。「ユーザ振舞い仕様」は、時間定数を明確にした段階でのMichonの「操作レベル」、「戦術レベル」である。また、「ユーザ振舞い仕様」はモデリング言語で記述した「ユーザモデル」である。
- (6) モデルベース開発ツール上の「ユーザモデル」は、モデルベース開発ツールで作られた「制御モデル」、「プラントモデル」、「シナリオ」とともにシミュレーションが可能な「ユーザ振舞い仕様」である。

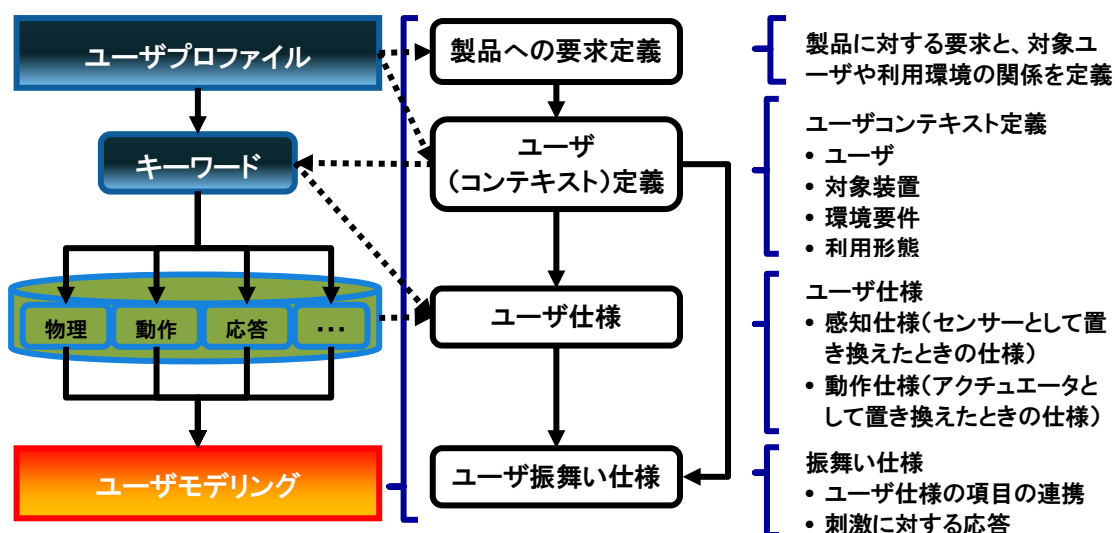


図 3-8 ユーザモデルの作成プロセス

3.4.2. 製品への要求定義

製品への要求定義では「製品に対する要求と、対象ユーザや利用環境の関係」を定義する。要求定義では製品と対象ユーザや利用環境の関係を定義することで、必要とされる利用時品質を定義し、製品設計に役立たせる。

記述方法としては、「SysML」による「ユースケース図」、「シーケンス図」、「クラス図」が考えられる。

3.4.3. ユーザコンテキスト定義

ユーザコンテキスト定義では「ユーザプロファイルと、製品への要求定義を基にユーザオペレーションを定義」する。その際には対象ユーザと対象装置・環境要件・利用形態の関係を定義する。

記述内容は、たとえば「横断歩道で、頭や目を動かしてまわりを視ている。」、「人の飛び出しを認知し、とっさにハンドルを切る」などのように、「環境を含む特定の刺激に対する応答が規定されたユーザ振舞いを定義」方法で行う。

具体的な記述方法は今後の課題となる。

3.4.4. ユーザ仕様

ユーザ仕様では「コンテキストに含まれるユーザの振舞い要素を抽出し、ユーザの認知や動作の値（式）を定義」する。コンテキストに含まれるユーザの振舞い要素はユーザプロファイルのキーワードであり、ユーザの振舞い要素の値または式はデータベースから抽出する。言い方を変えると、「ユーザのセンサー項目と値または式のセット」と「ユーザのアクチュエータ項目と値または式のセット」である。

ユーザの振舞い要素の記述内容は、たとえば「視野角」、「反射」、「首振り角」であり、ユーザの振舞い要素と値または式の記述内容は、「視野角=xx」、「反射=0.X秒」、「首振り角=X度」である。

具体的な記述方法は今後の課題となる。

3.4.5. ユーザ振舞い仕様

ユーザ振舞い仕様では、「ユーザ仕様の項目の連携（刺激に対する応答）を定義」する。ユーザ振舞い仕様はユーザコンテキスト定義とユーザ仕様を基に定義する。

ユーザ振舞い仕様を作成する際に重要なことは、ユーザコンテキストを、「シナリオ」と「ユーザ仕様の項目連携」に分離して定義し、「値または式」を記述する。

ユーザ振舞い仕様の記述内容は、たとえば「人の飛び出しを視野角=xx/首振り角=X度で認知し、反射=0.X秒でハンドルを切る」などのような内容である。

記述方法としては、「SysML」による「ユースケース図」、「シーケンス図」、「クラス図」が考えられる。

3.4.6. ユーザモデル

ユーザモデルは、シミュレーションが可能な「ユーザ振舞い仕様」であり、モデルベース開発ツールにおいて、「制御モデル」、「プラントモデル」、「シナリオ」とともに使う。ユーザモデルは、モデルベース開発ツールのプラントモデルと同様の形態で定義する。また、ユーザモデルを定義する際には、シナリオはユーザモデルとは独立に定義する。

3.5. 課題

本ユーザモデリング技術 WG で検討した「ユーザプロファイルを基にしたユーザモデルの作成」プロセスの実用化に向けては、「ユーザプロファイル」、「製品への要求定義」、「ユーザコンテキスト定義」、「ユーザ仕様」、「ユーザ振舞い仕様」、「ユーザモデル」等に関する詳細な定義を行う必要がある等、更に研究が必要である。

また 2011 年度の「ユーザモデリング調査」で判明した課題として、本プロセスの「ユーザ仕様」でユーザを定義する際に必要なユーザに関するデータが必要となるが、日本も他国においても公開情報が整備されているわけではないことが判明した。そこで、本ユーザモデリング技術 WG で検討したユーザモデルを採用する場合、当初はユーザ仕様に必要なデータベースも準備する必要がある。多様なユーザに対応する高い利用時品質を持つ製品の提供のためには、個別の企業レベルを超えてユーザに関わるデータベースを構築できるような仕組みが必要と考えられる。

4. 消費者機械安全標準化 PT

消費者機械とは、一般ユーザが利用する自動車、家電、サービスロボットなどの機械製品に対する造語である。これらは、多様な環境で多くのユーザに利用され、些細な不具合が深刻な事態を招くことがある。そこで、消費者機械の安全性・信頼性・セキュリティを含むディペンダビリティを保証するため、ソフトウェア開発に関する国際標準を消費者機械安全標準化 PT の活動を通して OMG に提案する。

4.1. 消費者機械の機能安全

消費者機械は表 4-1 に示すように、産業機械とは異なり、技術者の手を離れ、多様な環境で多くのユーザに利用される。些細な不具合が深刻な事態を招くことがあり、安全性と信頼性が特に重要である。しかしながら、現在の安全性に関する標準化の枠組みは ISO12100、ISO14121 や IEC61508 のような産業機械や工業プラントに対する安全の枠組みを拡大利用している。自動車やサービスロボットなどの領域で電子制御システムの機能安全規格が個別に制定されているが、消費者機械安全に対する標準化の枠組みは不十分である。さらに、開発中に悪意のあるコードが挿入される可能性を否定できない時代となり、情報ネットワークを通じて問題が深刻化する事態を想定せざるを得なくなっている。

	産業機械	消費者機械
生産数	a few ↔ many	a huge number
ユーザ	experts	general users
要求コスト	high	low
メンテナンス	現場 (strongly managed)	ユーザ、サービスステーション (weekly managed)
環境	工場環境 (ほぼ定常)	生産現場 ユーザ環境 (open, dynamic, and, diverse)

表 4-1 消費者機械と産業機械の違い

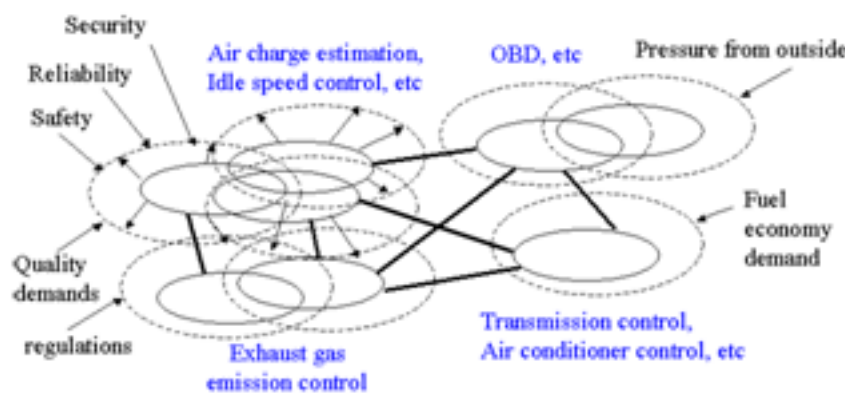


図 4-1 複雑システムとしてのエンジン制御

典型的な消費者機械である自動車は高い安全性と信頼性が求められるが、同時にクリーン化と気候変動への対応が求められ、自動車の制御システムは急速に複雑化している。自動車のエンジン制御だけでも、図 4-1 に示すように、筒内空気量推定、燃料噴射制御、点火時期制御、エンジントルク制御、排気ガスエミッション低減、異常診断などのシステムが複雑に絡み合っている。それぞれのシステムが各種の要求で独自に成長して行くので、製品の世代を超えて信頼性を保証し続けることは容易ではない。さらに、自動車は単体としての機能や効率向上を図ることは当然として、交通、配送、エネルギー供給、情報システムなどと連携して付加価値を創造する時代になっており、自動車制御システムは一層複雑化が進展すると予想される。このことは、ほとんど全ての消費者機械に当てはまる。

社会システムは図 4-2 に示すように交通、配送、エネルギー供給、情報システムなどが絡み合っただけで複雑なネットワークを構成している。ある時点での最適化だけではなく、長期間に渡る総合的な計画が極めて重要である。この構造は、先のエンジン制御システムと全く同じである。

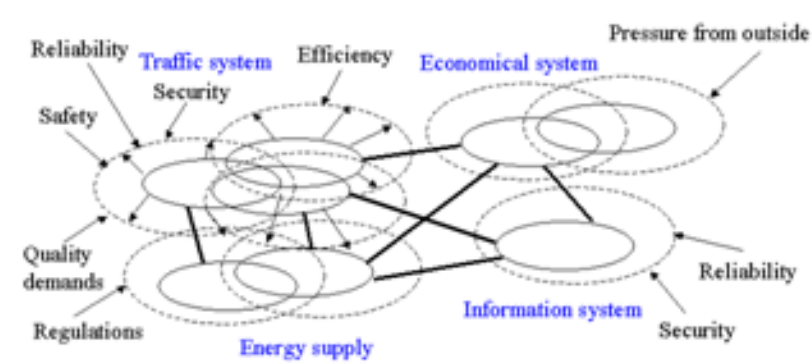


図 4-2 社会システムとの類似性

このような異種なシステムが組み合わされたシステムで世代を超えて管理しなければならないことは、今日の社会システムや製品開発に共通な課題である。消費者機械はそのような複雑なネットワークを構成する要素でもあり、些細な不具合が波及して、重大な社会問題を引き起こす可

能性を排除することはできない。すなわち、消費者機械の安全性、信頼性、セキュリティを含めたディペンダビリティを保証する枠組みを構築することは、今日の危急な課題である。

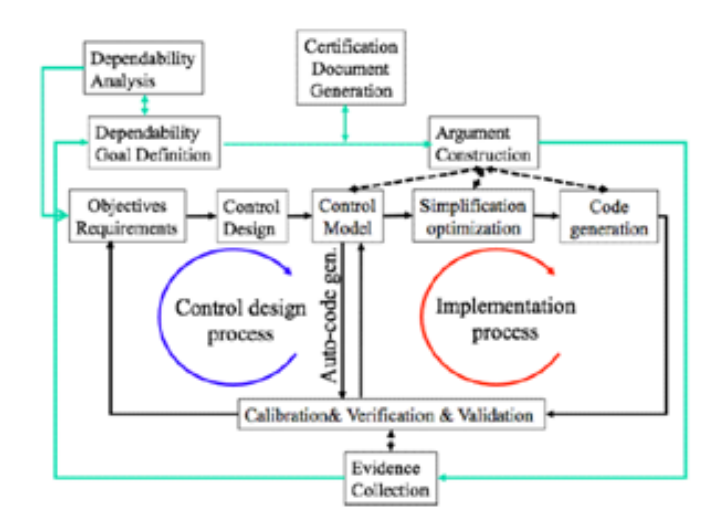


図 4-3 提案するプロセス

4.1.1. OMG 提案のオントロジモデル

委員から提案の全体像が分かり辛いという指摘があり、また今後必要となるであろう提案のメタモデルを作成するための足掛かりとして、OMG への提案の全体像を、コア（基本となる）概念の構造を明らかにするためのオントロジモデルとして見える化した。

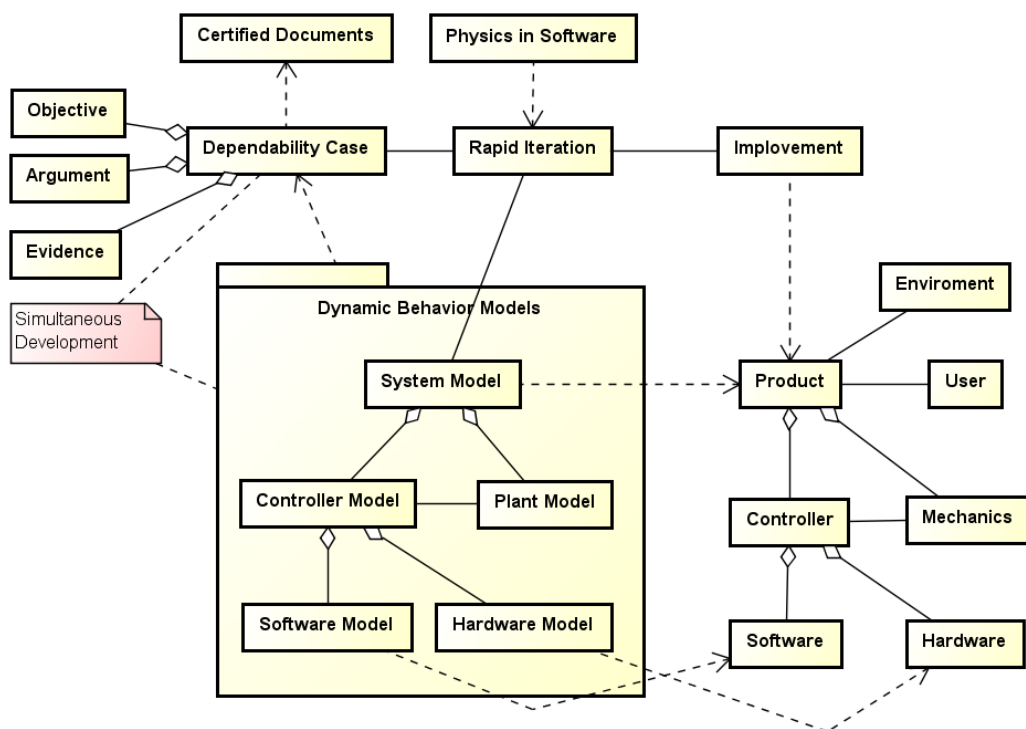


図 4-4 提案全体のオントロジモデル

ここでキー概念となるのは、「Rapid Iteration」、「Dynamic Behavior Models」、「Dependability Case」であり、それぞれの関係やその周辺の概念の関係を明確にしている。つまりオントロジモデルは、概念構成（提案に対するコア概念の構成）を明らかにすることはできるが、メタモデルのように標準化そのものをサポートするものではない。

4.2. 2011 年度の活動

- (1) IPA/SEC 消費者機械安全標準化セミナー（4/19@IPA 16F 大会議室）
- (2) 2011 年度 第 4 回 OMG (@サンタクララ)参加（12/13-17）
- (3) 第 1 回消費者機械安全標準化 PT 会議（12/28@IPA 13F A 会議室）
講師：(独) 産業技術総合研究所：田口 研治
東京大学： 松野 裕
- (4) 第 2 回消費者機械安全標準化 PT 会議
（1/12@東京大学情報基盤センター 3 階 大会議室）
講師：DEOSプロジェクト¹⁰：中川 雅通（パナソニック株式会社）
東京大学： 松野 裕
- (5) 第 3 回消費者機械安全標準化 PT 会議（2/15@IPA 13F B 会議室）
- (6) SEC journal（27 号）で「消費者機械安全性・信頼性保証の国際標準化」を発表した。

4.2.1. 活動内容

- (1) サンタクララで開催された 2011 年度第 4 回 OMG にて、消費者機械の Dependability 保証に関する RFI を System Assurance Task Force に提出し、12 月 14 日に認められた。12 月 16 日の OMG Board 会議にて OMG からの RFI として承認された（正式には Board 会議後の投票によるが、特別なことがない限り承認と見なされる。）。現在、OMG の Web サイトから RFI が公開されている。RFI のフィードバックの締め切りは 5 月 20 日である。

SysA/11-12-02-ADCD

RFI: Assuring Dependability of Consumer Devices: Automobiles,
Service Robots, Avionics, Smart Houses, etc. -

<http://www.omg.org/cgi-bin/doc?sysa/2011-12-02>

- (2) 第 1 回消費者機械安全標準化 PT では、情報共有とレベル合わせ。第 2 回 PT は推進体制と活動日程、消費者機械安全標準化のビジョン、第 3 回 PT では、ビジョンとスコープの継続

¹⁰ 「実用化を目指した組込みシステム用ディペンダブル・オペレーティングシステム」(DEOS (Dependable Embedded Operating Systems) プロジェクト)は、(独)科学技術振興機構(JST)/CREST の研究領域の 1 つとして、2006 年 10 月に開始された。DEOS は OSD (Open Systems Dependability) を実現するための知識・技術を体系だてたもの。CREST は JST の戦略的創造研究推進事業。

審議と 2012 年度活動に関して議論を行った。以下がそのまとめである。

- ① 本活動のビジョン:本 PT は Dependability Assurance に関する下記項目を包含する OMG 標準化を行う。
 - 消費者機械の Embedded control software と Dependability Cases の Simultaneous & Interactive Process (プロセスの対象: Dependability cases、Embedded control Software)
 - 動的振舞いモデルの利用 (微差分方程式で表された制御装置、制御ソフト、ソフトウェアに物理と数学を反映すること(Physics inSoftware))
 - 動的に変化する環境下における Dependability 保証
 - Human factors
 - 素早い繰り返しを実現する Dependability Cases と Embedded control software 開発の Formalization と Automation
 - 上記に基づくツールチェーンとツール間インターフェース

- ② OMG を通した消費者機械 Dependability 国際標準化の意義
 - 日本は高品質・高性能な消費者機械を合理的な価格で世界に提供してきた。日本の強みである高品質・高性能な消費者機械の Dependability 保証の方法を国際標準にする意義は大きい。
 - OMG は ISO の JTC1 とアライアンスを持っており、OMG 標準を ISO 化する場合は、影響力と OMG 標準化のスピードからメリットがあると考えられる (仮に ISO 化に時間を要しても、日本の強みを担保する標準が存在することに意義がある)。

- ③ アプローチ

ISO26262 をメタモデル化し、そこに(1)のビジョンで示す項目を加え、論理的矛盾のないプロセス、ツールチェーンを検討。続いて、この標準をサービスロボットなどの開発へ適用が可能な検証を行う。

- ④ OMG 標準化までの期間目標の設定

PT の成果をできるだけ、早い時期に出したい。これは、OMG を通した標準化の有効性の確認と続く標準化戦略を構築するために効果的であると考え。4 月 19 日の OMG 会長の Dr.Richard Mark Soley のリコメンドもあり、できるだけ早期の標準化を達成するため過去の実績等を踏まえ 18 ヶ月を標準化までの期間目標として設定する (以下、18 ヶ月 Target と略す)。

- ⑤ OMG 会長 Dr. Richard Mark Soley との計画整合性確認

OMG の標準化に際し、実装が求められるが、実際の Application での検証が不可欠であるとすると、多大な時間を要するので、18 ヶ月 Target は不可能なことになる。本件のケースでの実装の意味と 18 ヶ月 Target の OMG Policy との整合性を 3 月 1 日に OMG 会長の Dr. Richard Mark Soley と議論を行った。

- ▶ 18 ヶ月 Target は最短標準化日程期間(RFP 発行から)である。
- ▶ OMG は標準に矛盾がないことが重要であると考えており、そのための実装と位置づけをしている。
- ▶ 既存のケースでも矛盾がないことが示されれば、実際の Application で検証しなくてもよい。

この議論から、PT としては 18 ヶ月 Target を採用することにした。

⑥ DEOS プロジェクトとの連携

CREST「実用化を目指した組込みシステム用ディペンダブル・オペレーティングシステム」研究領域 (DEOS プロジェクト) と狙いを共有する部分があり、連携に関して議論を行ってきた。連携を検討することは合意されているが、具体的な連携内容に関しては今後調整が必要である。

4.3. 2012 年度に向けた活動提案

RFP 提案とそのフィードバックの提出により、OMG 標準化に向けて活動を継続する。2012 年度の活動計画を以下に示す。

- ① RFI フィードバック：消費者機械の Dependability 保証に興味を持つ個人、団体のフィードバックに対する制限はないが、IPA/SEC としてのフィードバックも行う必要がある。
- ② 消費者機械の Dependability 保証の国際標準化に向けて啓蒙活動の一環として、7 月にセミナーを開催する。
- ③ 最短での OMG 標準化のために、9 月の第 3 回 OMG 会議、または、12 月の第 4 回 OMG 会議に RFP 提案を行う。
- ④ RFP に対するフィードバックを RFP 発行後直ちに行う。
- ⑤ ISO26262 をメタモデル化し、Dependability Cases と Embedded Software n の同時開発、動的振舞いモデル、Physics in Software の概念を組み込み、RFP へのフィードバックを準備する。
- ⑥ 年 4 回の OMG 参加
- ⑦ DEOS プロジェクトとの連携の実現

4.4. おわりに

2011年度はOMGへの最初のアプローチを行い、RFIの発行を行うことができた。今後はRFIのレスポンスに対しての対応を行い、レスポンスしてくれた組織に協力を求めてRFPの提出を行う必要がある。PTで検討したスケジュールに対して、RFPはおそらく9月にドラフトを提出するに留まる可能性がある。つまりRFPの最終版は平成24年12月になると考えられる。

日本のモノ作りの良さがOMG標準として認められるかは、RFPの内容次第と言っても過言ではない。

5. 付録 部会・WG・PT の委員構成と実施内容

付録1 モデルベース開発技術部会

表 1-1 委員一覧(2012 年 3 月末時点)

表 1-2 実施内容

	実施時期	議題
第 1 回	2011 年 10 月 14 日	モデルベース開発技術部会の開催と各 WG に関する説明 ① モデルベース開発技術部会の概要 ② 各 WG の説明 (1) 統合システムモデリング技術 WG (2) ユーザモデリング技術 WG
第 2 回	2012 年 3 月 5 日	モデルベース開発技術部会の 2011 年度活動結果報告 ① 統合システムモデリング技術 WG 2011 年度活動報告と 2012 年度活動予定 (MBSE を検討する) ② ユーザモデリング技術 WG 2011 年度活動報告 ③ 消費者機械安全標準化 PT 2011 年度活動報告と 2012 年度活動予定

付録2 統合システムモデリング技術 WG

表 2-1 委員一覧(2012 年 3 月末時点)

	氏名(敬称略)	所属
主査	新 誠一	電気通信大学
委員	穴吹 雅敏	dSPACE Japan 株式会社
委員	阿部 睦	株式会社トヨタ IT 開発センター
委員	大西 建児	ガイオ・テクノロジー株式会社
委員	大畠 明	トヨタ自動車株式会社
委員	風間 博之	株式会社エヌ・ティ・ティ・データ
委員	金川 信康	株式会社日立製作所
委員	近藤 克之	富士通株式会社
委員	鈴木 万治	株式会社デンソー
委員	鈴木 尚志	日本アイ・ビー・エム株式会社
委員	中川 雅通	パナソニック株式会社
委員	中坊 嘉宏	独立行政法人産業技術総合研究所
委員	橋本 祐介	日本電気株式会社
委員	羽生田 栄一	株式会社豆蔵
委員	二上 貴夫	株式会社東陽テクニカ
委員	渡辺 政彦	キャッツ株式会社

表 2-2 実施内容

	実施時期	議題
第 1 回	2011 年 10 月 21 日	統合システムのリスクを整理 ① 統合システムモデリング技術 WG 活動計画案説明 ② 委員の自己紹介 ③ 講演：「消費者機械の安全性・信頼性を確保する開発技術と標準化」
第 2 回	2011 年 11 月 25 日	既存システムのリスクを低減するためのモデリング ① 講演：「モデル駆動システムズエンジニアリング」 ② MDD と MBD について討議
第 3 回	2011 年 12 月 20 日	統合システムのリスクを低減するためのモデリング手法を検討 ① 講演：「車載ソフトのモデリングとモデルベース開発環境の動向」 ② モデルとは ③ MDD と MBD について討議
第 4 回	2012 年 1 月 20 日	MDD と MBD の統合の検討 ① 講演：「ディペンダブルシステムのための Assurance Case」 ② 各自が考えるモデリング ③ MDD と MBD の統合について討議
第 5 回	2012 年 2 月 17 日	2011 年度のまとめ ① MDD と MBD の統合について検討結果発表 ② 報告書の検討 ③ 今後の予定について

付録3 ユーザモデリング技術 WG

表 3-1 委員一覧(2012 年 3 月末時点)

	氏名(敬称略)	所属
主査	山口 亨	公立大学法人首都大学東京
委員	穴吹 雅敏	dSPACE Japan 株式会社
委員	伊藤 隆文	株式会社デンソー
委員	鱈原 晴彦	株式会社 U' eyes Design
委員	大芝 英雄	株式会社ミクニ
委員	久保 孝行	アイシン・エイ・ダブリュ株式会社
委員	田村 政和	TIDA コンソーシアム/キャッツ株式会社
委員	中嶋 宏	オムロン株式会社
委員	西村 秀和	慶應義塾大学大学院
委員	久鍋 裕美	富士通デザイン株式会社
委員	古川 直広	株式会社日立製作所
委員	三島 隆司	東芝情報システム株式会社
委員	森江 信秀	アルパイン株式会社
委員	吉野 由紀夫	キャッツ株式会社

表 3-2 実施内容

	委員会開催実施時期	議題
第1回	2011年11月21日	ユーザプロファイリングとユーザモデリングの現状 ① 調査案件紹介：「利用者品質の確保に向けたユーザモデリング技術実用化調査」 ② 事例発表：「SysML による機能要求の分析と評価検証のためのモデリング」 ③ 議論1：「ユーザプロファイリングからの可能なアウトプット」 ④ 議論2：「ユーザモデリングへの可能なインプット」
第2回	2011年12月14日	ユーザモデルのためのモデリング技術 ① 調査中間報告：「利用者品質の確保に向けたユーザモデリング技術実用化調査」 ② 事例発表：「モデルベース開発におけるユーザモデル」 ③ 議論1：「ユーザプロファイルとユーザモデルの連携に必要な技術」 ④ 議論2：「ユーザプロファイリングに求められるアウトプット」 ⑤ 議論3：「ユーザモデリングに求められるインプット」
第3回	2012年01月11日	ユーザモデルを活用した開発プロセス ① 調査中間報告：「利用者品質の確保に向けたユーザモデリング技術実用化調査」 ② 事例発表1：「ユーザモデルに対する U' eyes Design の考え方」 ③ 事例発表2：「ユーザのモデル化技術に関する研究」 ④ 議論1：「ユーザプロファイルからのユーザモデル開発プロセス」
第4回	2012年02月10日	2011年度活動のまとめと2012年度の活動 ① WG 内調査最終報告：「利用者品質の確保に向けたユーザモデリング技術実用化調査」 ② 事例発表：「ドライバモデルを用いた運転動作評価に関する研究」 ③ 議論1：「ユーザプロファイルを基にしたユーザモデリングプロセス」 ④ 議論2：「報告書の方針」 ⑤ 議論3：「2012年度の活動」

付録4 消費者機械安全標準化 PT

表 4-1 委員一覧(2012年3月末時点)

	氏名(敬称略)	所属
主査	大島 明	IPA/トヨタ自動車株式会社
委員	秋山 進	株式会社デンソー
委員	金川 信康	株式会社日立製作所
委員	白坂 成功	慶應義塾大学大学院
委員	新 誠一	国立大学法人電気通信大学
委員	田口 研治	独立行政法人産業技術総合研究所
委員	中川 雅通	パナソニック株式会社
委員	中坊 嘉宏	独立行政法人産業技術総合研究所
委員	平鍋 健児	株式会社チェンジビジョン
委員	松野 裕	国立大学法人東京大学

表 4-2 実施内容

	委員会開催実施時期	議題
第1回	2011年12月28日	消費者機械の分類 ① WG 活動計画の説明 ② 委員自己紹介 ③ 講演 1:「ディペンダブルシステムのための Assurance Case」 ④ 講演 2:「OMG への RFI 提案について」 ⑤ 消費者機械について
第2回	2012年1月12日	消費者機械の安全性要件の整理 ① 講演:「DEOS プロジェクトの活動について」 ② RFI のレスポンスについて ③ 消費者機械の機能安全の標準化について討議
第3回	2012年2月15日	機能安全の標準化アプローチの検討 ① 消費者機械の機能安全の標準化について討議 ② 消費者機械安全標準化 PT 報告書(案)の検討 ③ 次年度の活動について