

組込みソフトウェアと形式手法

産業技術総合研究所

水口大知

内容

- 形式手法の適用事例ご紹介
- 北海道を中心とするサポイン事業ご紹介
- 簡易な形式文法による要求仕様記述ツールご紹介
- 名古屋地区での研究会ご紹介

ET 2010
出展中

形式手法の適用事例ご紹介

なぜ再び形式手法か？

- 高信頼性への要求が拡大している
 - テスト困難さが増大し、従来手法にはない検証能力が求められている
- 国際規格からの要請されている
 - IEC 61508 SIL 4
 - ISO/IEC 15408 (Common Criteria) EAL 7
- 支援ツール、検証ツールの性能が向上した
- 開発・保守コストの削減にもつながる
- UML等によりモデルの利用が普及した

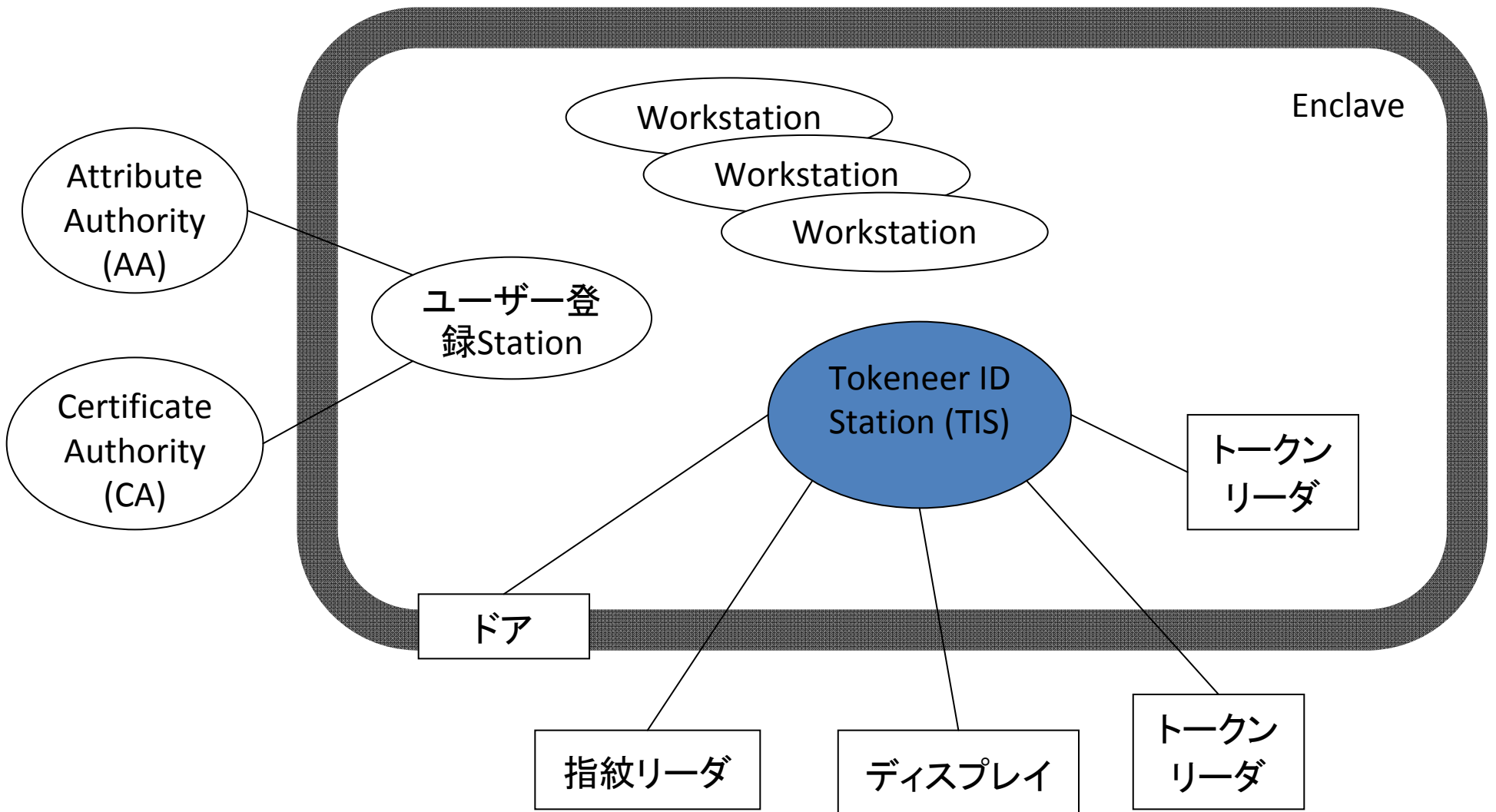
適用事例のひとつ

- “The Tokeneer Project”
 - <http://www.adacore.com/home/products/gnatpro/tokeneer/>
- 目的：EAL5に適合するシステムが、技術的・経済的に実現可能であることを示す
- National Security Agencyが依頼
- Praxis HISがSPRE Inc.と共同で実施
- Z記法による形式仕様記述、形式検証、段階的詳細化を含む
- 成果物を全て公開（2008年10月）

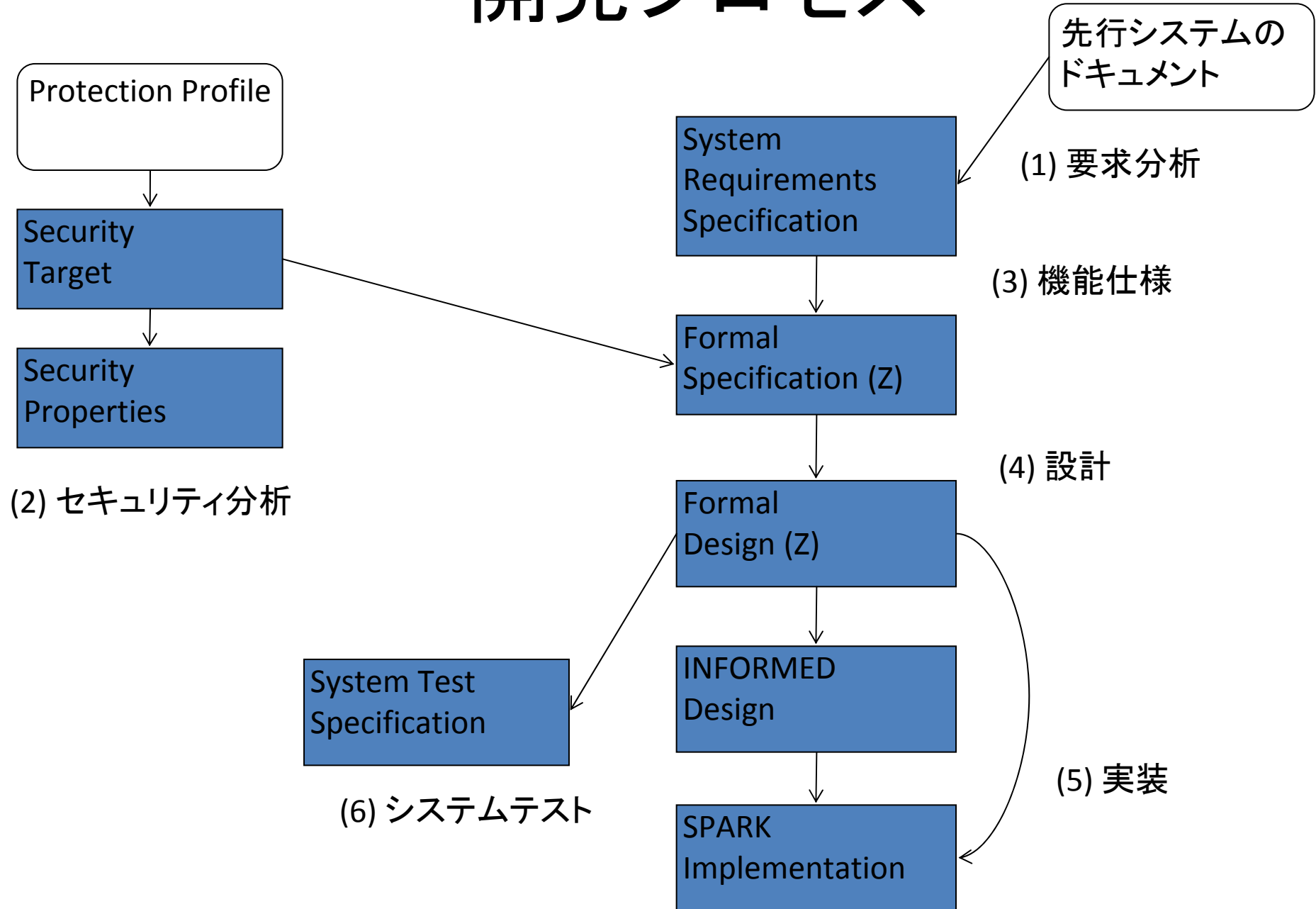
公開されているドキュメント

1. Project Plan
2. Protection Profile
3. Security Target
4. Approaching The Common Criteria
5. Summary of Security Target Exclusions
6. Security Properties
7. System Requirements Specification
8. Formal Functional Specification
9. Interface Specification
10. Formal Design
11. INFORMED Design
12. Code Verification Summary
13. System Test Specification
14. Fault Management Reports
15. Installation Guide and User Manual
16. Summary Report

Tokeneer システム & TIS



開発プロセス



保証活動

先行システムの ドキュメント

Protection Profile

Security Target

Security Properties

System Requirements Specification

Formal Specification (Z)

Formal Design (Z)

INFORMED Design

SPARK Implementation

Properties (Z)

Proof of Security Properties (SPARK)

System Test Specification

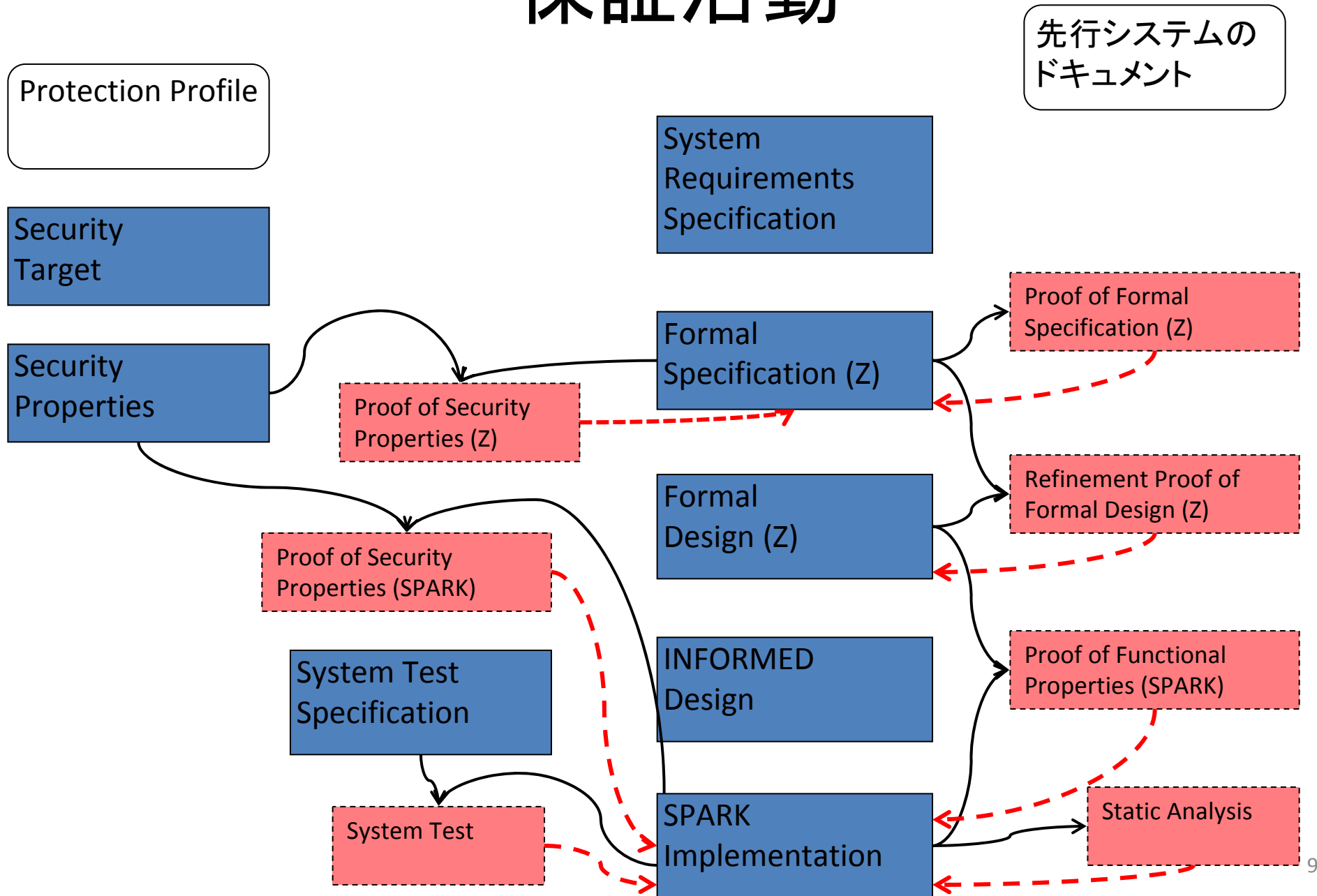
System Test

Proof of Formal Specification (Z)

Refinement Proof of Formal Design (Z)

Proof of Functional Properties (SPARK)

Static Analysis



事例のまとめ

- 『EAL5に従った開発プロセスに沿って、高品質かつコストに見合ったシステムを開発することができることを示した』
 - 『見逃したバグは1つ』
 - 『(Z記法やSPARK Adaといった)特定の技術のみに依拠するものではない』
 - 『あくまでも一例であり、Z記法でなければならないわけではない』
 - 『Z記法の利点: 曖昧さを含まない記述が可能、理解の確認・提示ができる、完全性・一貫性・セキュリティプロパティの証明が可能』

その他の事例

- 形式手法適用調査報告書、IPA、2010
 - http://www.ipa.go.jp/about/press/20100729_2.html
- Deploy
 - Industrial deployment of system engineering methods providing high dependability and productivity
 - an European Commission Information and Communication Technologies FP7 project
 - <http://www.deploy-project.eu/>



ET 2010
出展中

北海道を中心とするサポイン事業ご紹介

以下、北海道立総合研究機構 堀武司氏のスライドより抜粋
http://www.hkd.meti.go.jp/hokim/fm_seminar/result.htm

形式記述現場実践のための研究プロジェクトを開始！

- 経済産業省 (北海道経済産業局) 平成22年度戦略的基盤技術高度化支援事業
「形式的仕様記述を用いた高信頼ソフトウェア開発プロセスの研究とツール開発」(H22～24)

- 研究実施機関: 北海道を中心とする中小企業4社、北海道大学、産業技術総合研究所
- アドバイザ: 高信頼ソフトのニーズを持つ、北海道・中部地区の川上ユーザ企業、大学等



2010/08/27

2010 Sapporo

40

戦略的基盤技術高度化支援事業（サポイン事業）

- 経済産業省の委託事業
 - － 「川上」企業と「川下」企業が連携して、中小企業のものづくり基盤技術を高度化し、製造業の国際競争力強化と新たな事業の創出を促進する事を目的とする。
- 川上企業（研究実施の主体）
 - － ものづくり技術を持つ中小企業
- 川下企業（アドバイザー等として参画）
 - － 川上企業の要素を利用し、製品の製造を行うメーカー（例：自動車メーカーなど）

当場の形式手法への取り組みのきっかけ

- 「機能安全対応自動車制御用プラットフォームの開発」
 - － 経済産業省 戦略的基盤技術高度化支援事業 (H18～21)
 - － 参画機関
 - 研究実施機関: (株)ヴィッツ、(株)サニー技研、東海ソフト(株)、名古屋大学、産業技術総合研究所、名古屋市工業研究所、北海道立工業試験場
 - － **IEC 61508 安全度水準 SIL3** に対応した自動車制御用OS、車載通信ミドルウェア(CAN, LIN, FlexRay)の開発
 - － (副次効果として) 機能安全規格に対応出来る企業、機関、人材の育成
- 機能安全国際規格 IEC 61508 (JIS C0508)とは…
 - － 「電気・電子・プログラマブル電子安全関連系の機能安全」
 - － ヨーロッパ主導で、西暦2000年に発行
 - － ハード+ソフトで実現される安全系に関する規格
 - － 対象分野: 産業機器、プラント制御、自動車、鉄道など

IEC 61508 と形式手法

- IEC 61508では、機能安全対応ソフトウェア開発における推奨手法の一つとして形式手法が位置付けられている。
 - IEC61508-3 表A.1, 表A.2, 表A.4, 表A.9, 表B.5, 表B.7参照
 - **SIL4 では、形式手法の使用が「必須」**
- 具体的な手法の選定や活用方策までは、規格では言及していない。
- (自動車向けでは必須ではないが)将来的なSIL4対応を視野に入れ、形式手法に関しても調査を行う事となった。

IEC 61508-3 表A.1 ソフトウェア安全要求仕様(7.2参照)

	技術／手法	SIL1	SIL2	SIL3	SIL4
1	コンピュータ支援による仕様書作成ツール	R	R	HR	HR
2 a	半形式的手法	R	R	HR	HR
2 b	形式的手法 (CCS, CSP, HOL, LOTOS, OBJ, 時相論理, VDM及びZ 等を含む)	—	R	R	HR

HR（強い推奨）では、2 a、2 bのどちらかを選択

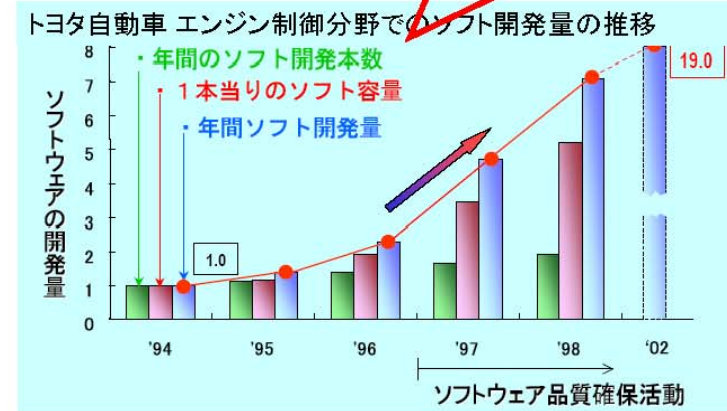
組込みソフトの課題：開発規模の爆発と不具合比率

我が国が得意とする組込み機器開発において、電子装置開発、特に組込みソフトウェア開発規模は爆発的に増大し（8年で19倍）、そのため、ソフトウェアの品質維持が困難となりつつある。

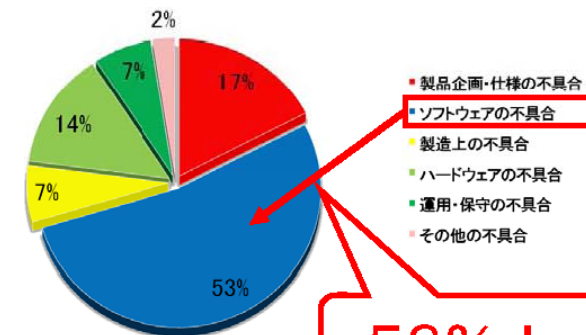
組込み製品の不具合比率では、ソフトウェアの不具合が53%を占める。

組込みソフトウェアに起因する重大故障が大きな社会問題となりつつある。

8年で19倍！



組込み製品の不具合原因比率



ソフトウェア不具合の原因

● 信頼性が低下する原因

要求仕様の問題

要求仕様の不具合原因は？

あいまい性、矛盾を含んでいる

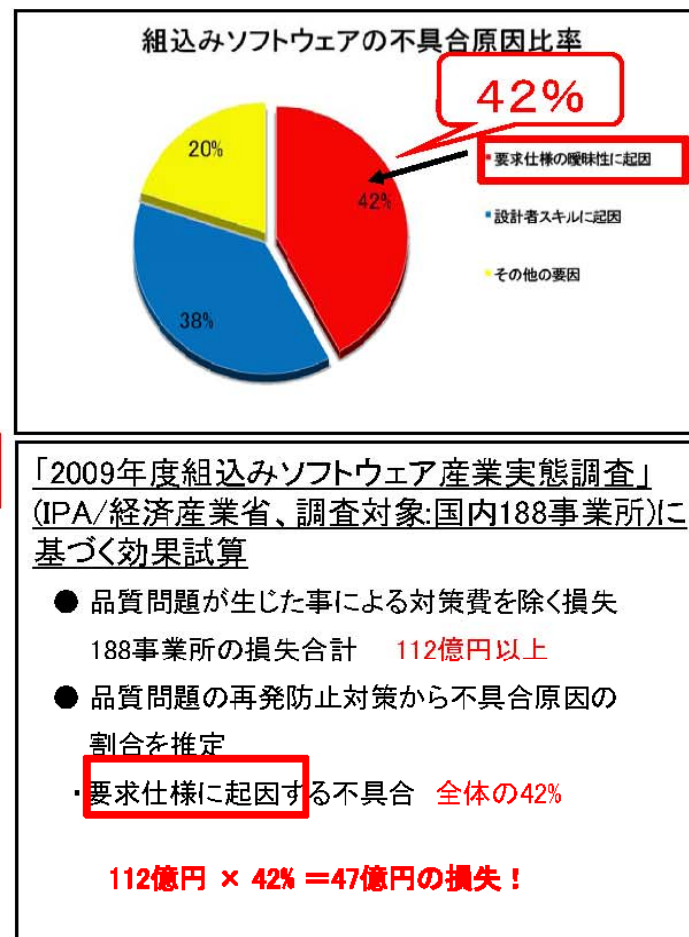
不具合の42%を占める！

この対策を行うことが1番効果的

● なぜ、あいまいになるのか？

厳密な意味が定義されない自然言語の使用が一因

解決法として、**形式的仕様記述**が注目されている。



研究の実施内容・方針

● 実開発に近いプロジェクトを対象に 形式手法の試験導入

- ・自動車部品用組込み制御ソフト
(自動車部品メーカーから情報提供)
- ・通信プロトコル
(TCP/IPプロトコルスタック)

● どの様に？

形式的仕様記述による再開発

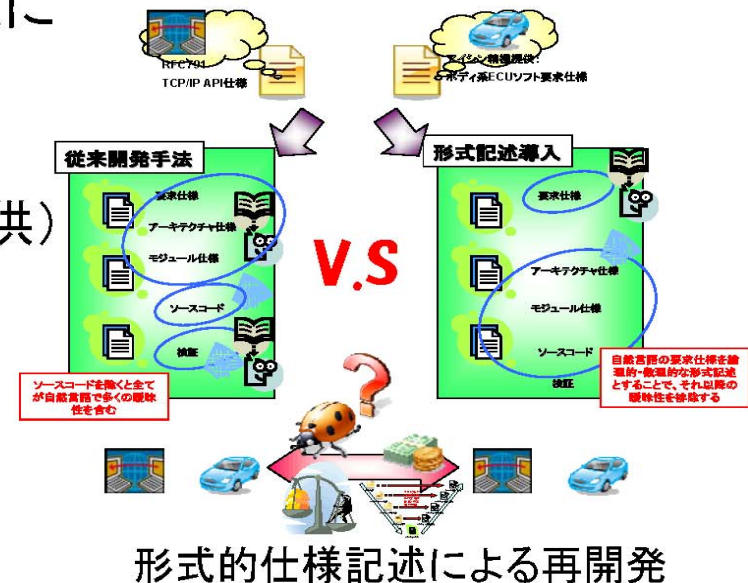
従来手法開発との比較・分析

有効性の検証

形式的仕様記述の
開発プロセスを確立

ツール・教材の開発

形式的仕様記述を
広く普及させるために



2010/08/27

フォーマルメソッド普及促進セミナー
2010 Sapporo

44

B抽象機械に基本的な記法

MACHINE 機械名称 (パラメータ, ...)

VARIABLES

変数名, ...

INVARIANT

変数の型宣言 &
抽象機械の不変条件

INITIALISATION

変数の初期化处理

OPERATIONS

出力変数 ← 操作1 (パラメータ, ...) =
PRE 事前条件 THEN
操作の処理内容

END

END

出力変数 ← 操作2 (パラメータ, ...)

...

END

● 抽象機械

- 状態 + 操作をカプセル化したもの (OOPのクラス定義に類似)
- 状態: 状態変数で表現
- 操作: 状態変数の書き換え規則

● プログラムと違う点

- 事前条件: 操作の実行時に満たされるべき条件
- 不変条件: 抽象機械の状態が常に満たしているべき条件

簡単なB抽象機械の記述例

Booking (座席予約)

```
MACHINE Booking (max_seat)
CONSTRAINT
    max_seat  $\in$  NAT

VARIABLES
    seat                // 残り座席数

INVARIANT
    seat  $\in$  0 .. max_seat // 整数の部分集合であり
                          // 0~max_seatの値をとる

INITIALISATION
    seat := max_seat

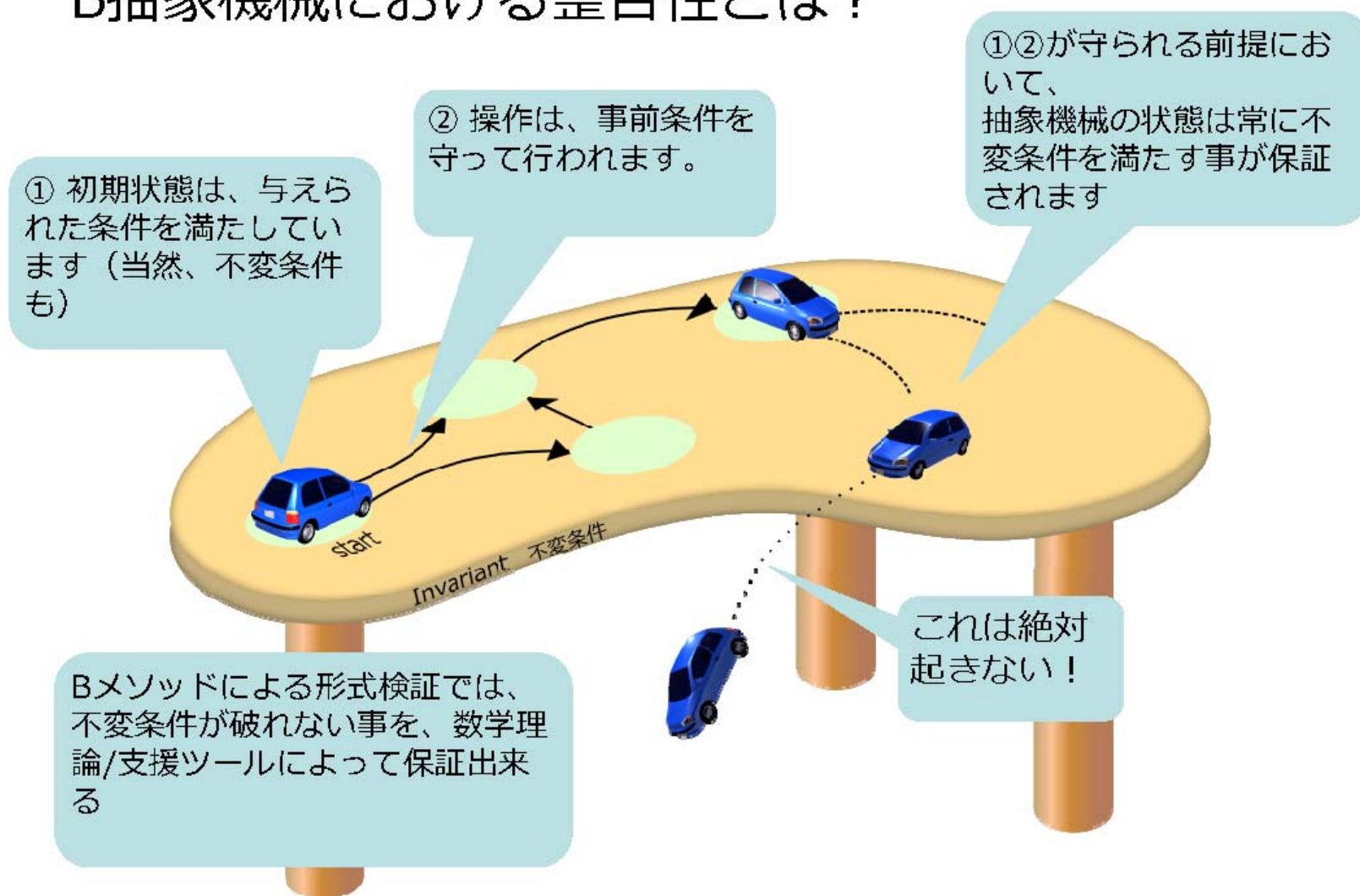
OPERATIONS
    book = PRE 0 < seat THEN // 座席が1以上なら予約可
        seat := seat - 1
    END;

    cancel = PRE seat < max_seat THEN
        // 最大数以上は返却不可
        seat := seat + 1
    END

END
```

- 概要
 - 座席の予約、キャンセル
 - 状態
 - 残り座席数
 - 操作
 - 予約する book
 - キャンセル cancel
- 集合論と論理に基づく記述
 - 一見ただのプログラム言語のように見えるが...
 - 条件式: **述語論理式**
 - 処理文: **一般化代入文**
 - 数学理論に基づく検証が可能

B抽象機械における整合性とは？



2010/08/27

フォーラムメソッド普及促進セミナー
2010 Sapporo

24

不変条件の重要性

- Bメソッドの整合性検証では、不変条件として記述した条件が検証される。
 - assertion や テストよりも、強力で網羅的な検証が可能。
 - しかし、不変条件として記述しなければ検証出来ない。
- 表現したい仕様を、いかにして不変条件に盛り込むか、がBメソッドによる仕様記述のポイントである。

検証方法

- 定理証明による方法

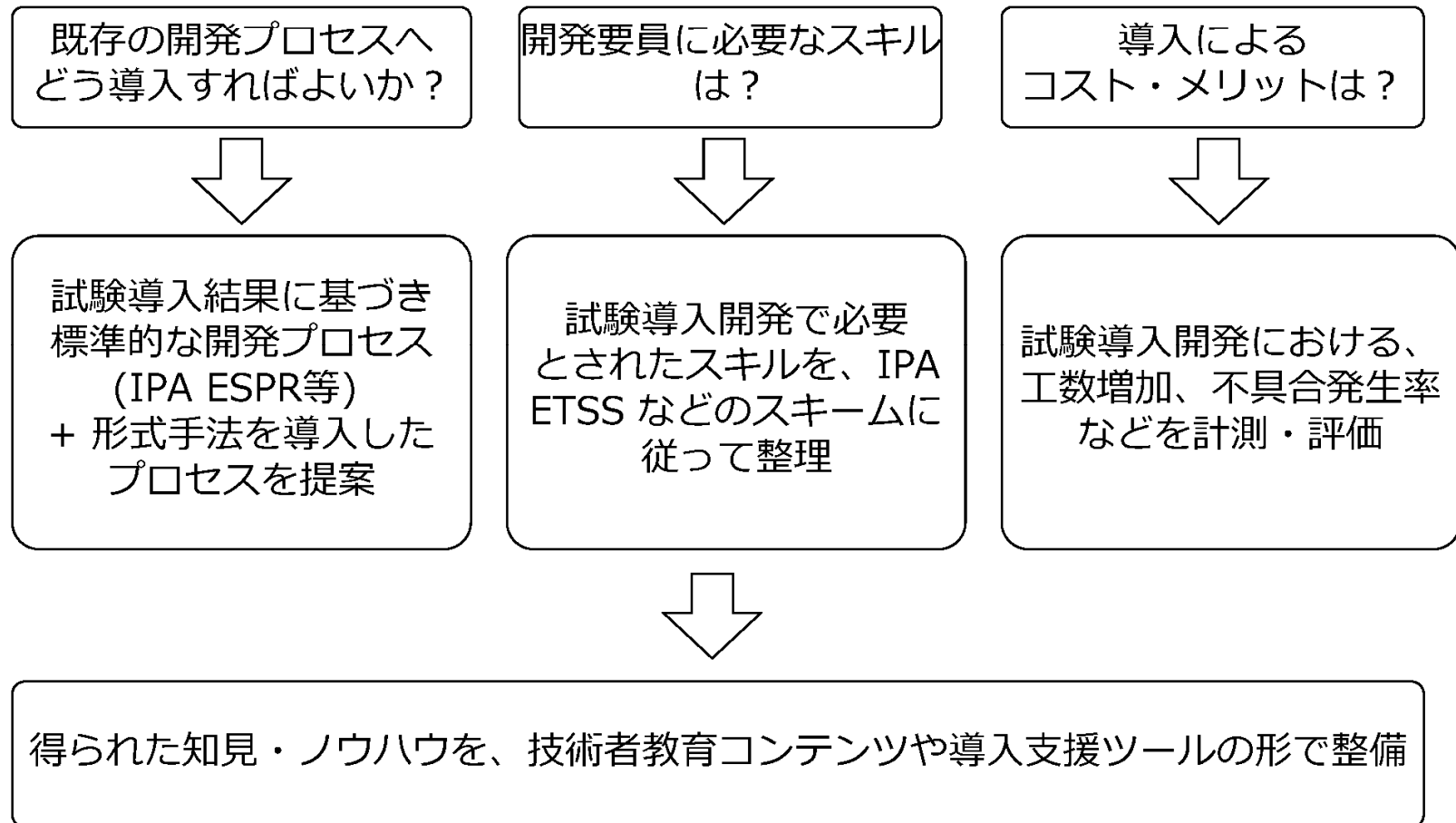
- 仕様記述から、「証明責務」(Proof Obligation)とよばれる証明問題を生成
- POを全て証明 → 仕様の整合性が示される。
- 証明作業は、手作業または自動定理証明器で行う。
- 検証作業には、専門知識と工数が必要

- モデル検査による方法

- 状態空間を網羅的に探索し、不変条件が偽になる状態がないか調べる。
- 検証作業はツールによる自動実行。
- 状態空間が広い、または無限の場合、検証作業は困難になる。

- Bメソッドでは、両方のツールが提供されている。

形式手法の現場導入の課題を解決



北海道を形式手法実践の先進地域に！

経済産業省北海道経済産業局
「平成22年度 情報政策の重点取り組みについて」より

主要な取組

<1>モバイルコンテンツビジネスの振興

業界の組織化支援、東京ゲームショウへの出展や全国各地の関係者によるサミットを開催。

<2>組込ソフトウェアの信頼性確保に向けた新技術・高度化支援

「形式手法」の普及促進。

<3>クラウドコンピューティング※に対応した地域ビジネスモデルの構築支援

クラウドコンピューティングのビジネスモデルの調査・検討。

※ 利用者がソフトウェア等のシステムを自ら保有するのではなくインターネットを通じてサービスとして利用する新たなコンピュータの利用形態。

<4>地域産業(特に食関連)の潜在的ニーズ掘り起こしとマッチング

- ・地域産業(特に食関連)の課題や経営効率化の動向等を関係業界等から「発掘」し、IT活用事例を活用したセミナーやグループスタディを開催。
- ・ITコーディネータによるコンサルティング、ユーザーとIT企業のビジネスマッチングによるIT導入の「実践」。
- ・表彰制度を活用した「成功事例の見える化」。



国内の形式手法取り組みは、まだ本格化していない状況

他地域に先駆けた取り組みによって、「形式手法は北海道」というブランドを確立し、高信頼ソフト分野への道内企業の参入を進めたい！

ET 2010
出展中

簡易な形式文法による要求仕様記述ツールご紹介

～ SLPによる組込みシステム要求仕様書のレビュー ～

SLPお問い合わせ

株式会社ジェーエフピー

<http://www.jfp.co.jp/slp/index.htm>

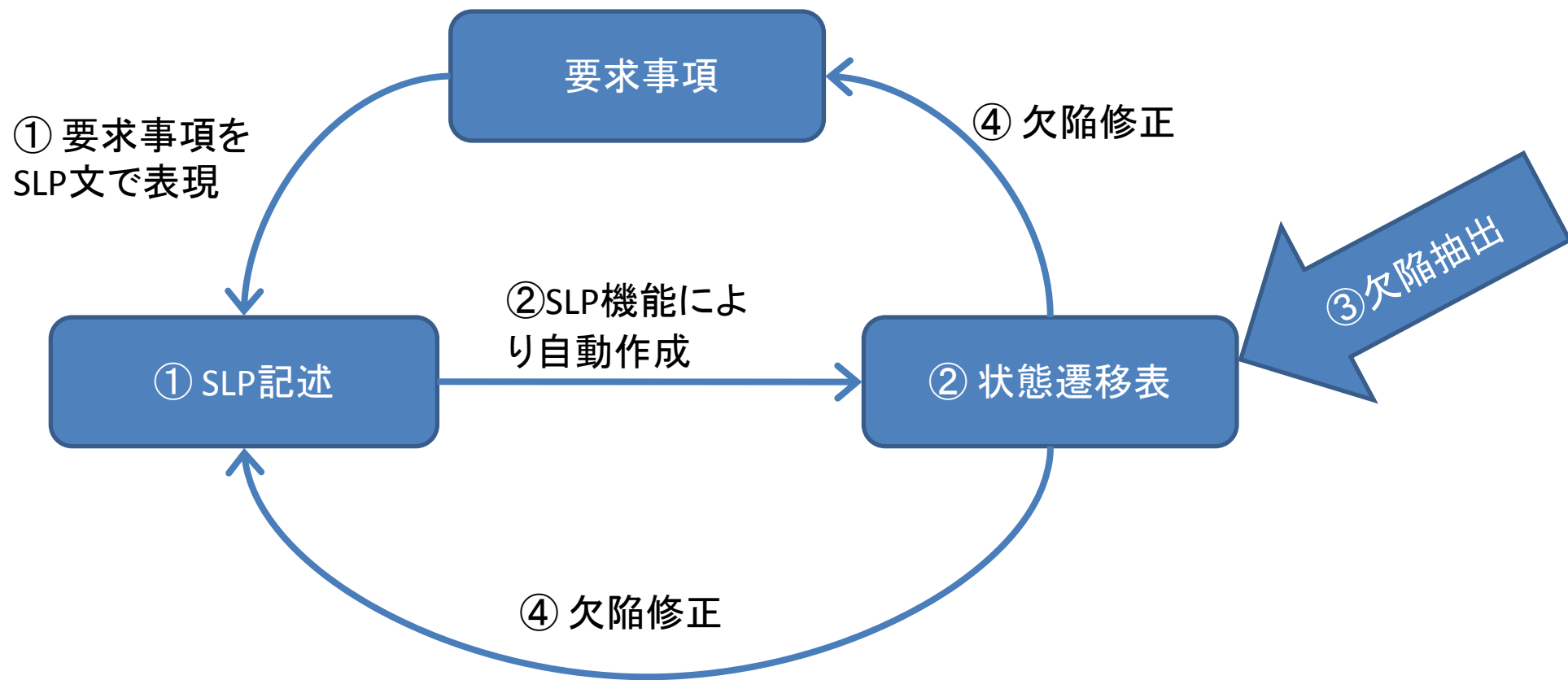
100日間試用版がDLできます

要旨

- SLPを用いて要求仕様書を書くと、レビューを効率的に行うことができます
 - SLPで記述するだけで、主語のもれや、場合分けのもれに気づくことができます
 - 状態遷移表を活用することで、論理的な整合性の誤りを効率的に発見することができます

レビューの手順

- ① 要求事項をSLPで記述する
- ② SLPで状態遷移表を作成する
- ③ 状態遷移表を眺めて、おかしいところを見つける
- ④ 要求事項およびSLP記述を修正する(①へ)



適用事例の紹介

- 「話題沸騰ポット 要求仕様書 第7版」に、レビュー手順を適用してみた
- 109件の指摘事項がでてきた

指摘事項の分類

	分類	指摘箇所の数
メンバー名	メンバー名もれ	22
	メンバー名表記のゆれ	11
状態名	状態名表記のゆれ	19
	状態もれ	8
状態遷移の条件	条件もれ	24
	余計な条件	3
	煩雑な条件記述	5
	条件にあらわれるメンバー名のゆれ	6
状態遷移	余計な状態遷移	6
	状態遷移もれ	3
	状態遷移の非決定性	2
		計 109

題材について

- 「話題沸騰ポット 要求仕様書 第7版」
- 一般的な電気ポットを想定した要求仕様書
 - 教材として、組込みソフトウェア管理者・技術者育成研究会 (SESSAME) より配布されている
 - http://www.sesame.jp/workinggroup/WorkingGroup2/POT_Specification.htm よりダウンロード可能

- 仕様書の目次は以下の通り
 1. ハードウェア構成とハードウェア要求仕様
 - 外観と内部構成、操作パネル部
 2. 操作要求仕様
 - コンセント、蓋、沸騰ボタン、保温設定ボタン、解除ボタン、給湯ボタン、タイマボタン、水位メータ
 3. 温度制御行為
 - 沸騰行為、保温行為、温度制御行為をしない(アイドル)
 4. 温度制御方式
 5. エラー検知
 6. 状態遷移
 - 話題沸騰ポット状態遷移図、話題沸騰ポット状態遷移表
 7. イベント

①SLPで記述する

- もとの仕様書の目次を踏襲して、階層的に記述した
 - もとの要求事項を、ひとつのFnとして記述した
- 原文の内容の通りに記述した
- 条件分岐に注目して記述した
 - 細かなところはそのままDo構文の状態名とした

SLP記述例

要求番号	pot-330-41
原文	アイドル中に蓋センサonとなったら、沸騰行為に遷移する。
SLP記述	<pre>if <ポットの状態>{アイドル中} if <蓋センサ>{on} Do<ポットの状態>{沸騰行為にせよ} else next endif else next endif</pre> SLPで記述するだけで、 記述もれが指摘できる
指摘・修正 事項	・「アイドル」、「沸騰行為」の主語が明記されていないので、「ポットの状態」を明記する。
分類	・メンバー名もれ

- 0 話題沸騰ポット第7版
 - 1 ハードウェア構成とハードウェア要求仕様
 - 2 操作要求仕様
 - 2.1 コンセント
 - 2.1.1 プラグの抜き差し
 - 2.2 蓋
 - 2.2.1 蓋を閉じたら
 - 2.2.1.1 蓋「閉」を確認する
 - 2.2.1.2 水量適正時の処理
 - 2.2.1.3 水量異常時の処理
 - 2.2.2 蓋を開けたら
 - 2.3 沸騰ボタン
 - 2.3.1 再沸騰
 - 2.3.1.1 沸騰ボタンが有効な時
 - 2.3.1.2 沸騰ボタンが無効な時
 - 2.4 保温設定ボタン
 - 2.4.1 保温設定
 - 2.4.1.1 デフォルト（保温モード）
 - 2.4.1.2 モード切換え
 - 2.4.1.3 保温温度設定
 - 2.4.1.4 モード表示
 - 2.5 解除ボタン
 - 2.5.1 ロック／ロック解除
 - 2.5.1.1 デフォルト（給湯口ロック）
 - 2.5.1.2 解除ボタンが有効な時
 - 2.5.1.3 解除ボタンが無効な時
 - 2.6 給湯ボタン
 - 2.6.1 給湯
 - 2.6.1.1 ポンプを作動できる場合
 - 2.6.1.2 途中でポンプを停止する場合
 - 2.7 タイマボタン
 - 2.7.1 タイマの起動
 - 2.7.1.1 デフォルト（タイマ）
 - 2.7.1.2 タイマ値のセット
 - 2.7.1.3 タイマ値をセットする時の操作音
 - 2.7.1.4 タイマの始動
 - 2.7.1.5 タイマ始動後のタイマ値の表示
 - 2.7.1.6 蓋「開」時に有効な操作
 - 2.7.2 タイマの停止
 - 2.7.3 タイムアップ時
 - 2.8 水位メータ
 - 2.8.1 水量表示
 - 2.8.1.1 水量異常の判断

SLP記述の目次(一部)

②状態遷移表を作る

- SLPのメニューから、
「プロセス」→「デシジョンテーブル作成」
を選ぶと、状態遷移表が得られる
(Do構文にかかるif節の条件を集めて、メンバー名毎に
集めたもの)

●蓋	蓋センサ							
閉じられたにせよ	3sec以上on							
●ポットの状態	蓋	水量	沸騰ボタン	ポットの状態	ブザー	プラグ	蓋センサ	全ての水位センサ
沸騰行為にせよ	閉じられた	適正	—	—	—	—	—	—
沸騰行為にせよ	—	—	100msec以上押された	保温行為中 ∧ ~給湯中	[100msec鳴らせ]	—	—	—
沸騰行為にせよ	—	—	—	アイドル中	—	—	on	—
保温行為にせよ	—	—	—	カルキ抜き加熱を終えた	—	—	—	—
アイドルにせよ	—	—	—	—	—	つながれた	—	—
アイドルにせよ	—	—	—	(保温行為中) V (沸騰行為中)	—	—	off	—
アイドルにせよ	—	—	—	(保温行為中) V (沸騰行為中)	—	—	—	off
●温度制御行為	蓋センサ							
中止せよ	1sec以上offとなった							
●すべてのインジケータセルランプ	蓋センサ							
消灯せよ	1sec以上offとなった							
●給湯口	蓋センサ	給湯口	プラグ	解除ボタン	ポットの状態			
ロック解除せよ	1sec以上offとなった	ロックされている	—	—	—			
ロック解除せよ	—	—	つながれた	—	—			
ロック解除せよ	on	ロック中	—	100msec以上押された	~給湯中			
ロックせよ	on	~ロック中 ∧ ロック解除中	—	100msec以上押された	~給湯中			
●ロックランプ	蓋センサ	給湯口	解除ボタン	ポットの状態				
消灯せよ	1sec以上offとなった	ロックされている	—	—				
消灯せよ	on	ロック中	100msec以上押された	~給湯中				
...	...	...	...	...	...	...	...	...

初期の状態遷移表(一部)

③おかしいところを見つける

- 基本的には、状態遷移表の遷移条件を一行一行チェックしていった
 - 間違いはないか？
 - 改善の余地はないか？

例えば、

●ポットの状態	蓋	水量	沸騰ボタン	ポットの状態	ブザー	プラグ	蓋センサ	全ての水位センサ
沸騰行為にせよ	閉じられた	適正	Don't Care	Don't Care	—	—	—	—
沸騰行為にせよ	—	—	100msec以上押された	保温行為中へ〜給湯中	[100msec鳴らせ]	—	—	—
沸騰行為にせよ	—	—	—	アイドル中	—	—	on	—
保温行為にせよ	—	—	—	カルキ抜き加熱を終えた	—	—	—	—
アイドルにせよ	—	—	—	Don't Care	—	コンセントにつながれた	—	—
アイドルにせよ	—	—	—	(保温行為中) V (沸騰行為中)	—	—	—	off
...	...	...	...	...	「ポットの状態」をながめてみると・・・			

指摘例1

●ポットの状態	蓋	水量	沸騰ボタン	ポットの状態	ブザー	プラグ	蓋センサ	全ての水位センサ
沸騰行為にせよ	閉じられた	適正	Don't Care	Don't Care	—	—	—	—
沸騰行為にせよ	—	—	100msec以上押された	保温行為中へ～給湯中	[100msec鳴らせ]	—	—	—
沸騰行為にせよ	—	—	Don't Care	アイドル中	—	—	on	—
保温行為にせよ	—	—	Don't Care	カルキ抜き加え終わった	—	—	—	—
アイドルにせよ	—	—	Don't Care	—	—	—	—	—
アイドルにせよ	—	—	Don't Care	—	—	—	—	off
...	...	...	...	...	...	...	...	...

ここでは「水量」が「—」となっているが、
 2行前では、「水量」が「適正」が条件と
 なっている！！
 ⇒ここは条件もれでは？？
 ⇒ pot-330-41の条件もれを確認。

指摘例2

●ポットの状態	蓋	水量	沸騰ボタン	ポットの状態	ブザー	プラグ	蓋センサ	全ての水位センサ
沸騰行為にせよ	閉じられた	適正	Don't Care	Don't Care	—	—	—	—
沸騰行為にせよ	—		100msec以上押された	保温行為中へ〜給湯中	[100msec鳴らせ]	—	—	—
沸騰行為にせよ	—	—	—	アイドル中	—	—	on	—
保温行為にせよ	—	—	—	カルキ抜き加熱を終えた	—	—	—	—
アイドルにせよ	—	—	Don't	—	—	コンセン	—	—
アイドルにせよ	—	—	—	—	—	につな	—	off
...	...	...	...	...	...	...	...	...

蓋に関する条件が、異なるメンバー名により表現されている！！
⇒メンバー名がゆれているのでは？
⇒ pot-330-41の条件を、「蓋センサがon」から、「蓋が閉」に修正。

指摘例3

●ポットの状態	蓋	水量	沸騰ボタン	ポットの状態	ブザー	プラグ	蓋センサ	全ての水位センサ
沸騰行為にせよ	閉じられた	適正	Don't Care	Don't Care	—	—	—	—
沸騰行為にせよ	—	—	100msec以上押された	保温行為中へ給湯中	[100msec鳴らせ]	—	—	—
沸騰行為にせよ	—	—	—	アイドル中	—	—	on	—
保温行為にせよ	—	—	—	沸騰ボタンを抜き加えた	—	—	—	—
アイドルにせよ	—	—	—	「沸騰」ボタンを押した	—	コンセン	—	—
アイドルにせよ	—	—	—	「保温」ボタンを押した	—	—	—	off
...	...	...	...	...	...	...	...	...

水量に関する条件が、異なるメンバー名により表現されている！！
 ⇒メンバー名がゆれているのでは??
 ⇒ pot-330-12, pot-330-13 の条件を、「全ての水位センサがoff」から、「蓋が空」に修正。

④要求事項・SPL記述を修正する

- 指摘事項を解消するための修正を、要求事項およびSLP記述に対して行った
- レビューと修正の反復を31回行った

要求番号	pot-330-41
原文	アイドル中に蓋センサonとなったら、沸騰行為に遷移する。
SLP記述 (修正後)	<pre> if <ポットの状態>{アイドル中} if <蓋>{閉} if <水量>{適正} Do<ポットの状態>{沸騰行為中にせよ} else next endif else next endif else next endif </pre>
指摘・修正 事項	・「アイドル」、「沸騰行為」の主語が明記されていないので、「ポットの状態」を明記する。 ・「蓋センサon」とあるが、pot-220-11では「蓋センサが3sec以上on」とあり、条件記述がゆれている。そこで、後者(つまり蓋が閉)に統一する。 ・原文では水量の条件が述べられていないが、pot-330-12、pot-330-13ではアイドルとなる条件に「水量が空」であることが述べられており、整合していない。ここでは条件に「水量が適正」であることも必要であり、明記する。
分類	・メンバー名もれ ・状態名表記のゆれ & 条件にあらわれるメンバー名のゆれ ・条件もれ

指摘例1および指摘例2に基づく修正

反復修正後の「ポットの状態」(一部)

●ポットの状態	ポットの状態	蓋	水量	沸騰ボタン	ポンプ	ブザー	水温	ヒータ	プラグ
沸騰行為にせよ	アイドル中	閉	適正	—	—	—	—	—	—
沸騰行為にせよ	保温行為中	—	—	100msec 以上押 された	~給湯中	[100msec 鳴らせ]	—	—	—
保温行為にせよ	沸騰行為中	—	—	—	—	—	100℃に なった	[カルキ 抜き]	—
アイドルにせよ	—	—	—	—	—	—	—	—	コンセ ントに つなが れた
アイドルにせよ	(保温行為 中) V (沸騰行 為中)	—	空	—	—	—	—	—	—
温度エラーにせ よ	—	—	—	—	—	—	110℃を 超えた	—	—
...	...	...	...	...	...	...	...	...	...

レビューのポイント

- 表現はゆれていないか？
- 条件はもれていないか？
 - 他の要件で参照されているメンバー名は考慮しなくてよいか？
- 条件は簡単にならないか？
 - 余計な条件はないか？
 - メンバー名を統一できないか？
 - 状態遷移表はコンパクトにならないか？
- 状態はもれていないか？
 - 未定義状態が参照されていないか？
- 状態遷移はもれていないか？
 - 場合分けの考慮もれはないか？
 - 遷移に非決定性が生じていないか？

SLPによるレビューの利点

役割分担

“部分”

```
if <ポットの状態>{アイドル}  
  if <蓋センサ>{on}  
    Do<状態>{沸騰行為にせよ}  
  else  
    next  
  endif  
else  
  next  
endif
```

ローカルな振る舞いを記述する

“全体”

●ポットの 状態	ポットの状態	蓋	水量	沸騰ボタン
沸騰行為 にせよ	アイドル中	閉	適正	—
沸騰行為 にせよ	保温行為中	—	—	100msec以 上押された
保温行為 にせよ	沸騰行為中	—	—	—
アイドルに せよ	—	—	—	—

グローバルな整合性を確認する

ET 2010
出展中

名古屋地区での研究会ご紹介

組込みシステム形式手法研究会

背景

近年、様々な製品にコンピュータが組込まれ、搭載されるソフトウェアの規模は増加傾向にあります。また、開発コストの中でソフトウェア開発の占める割合も高くなっており、ソフトウェア開発の生産性が大きな課題となっています。そして、コンピュータシステムに求められる複雑な動作を迅速に、そして、正しく実現するための開発技術が求められています。

形式手法とは

形式手法とは、数学的理論を背景にしたシステムの設計及び検証の手法のことで、形式手法またはフォーマルメソッド (Formal Method) と呼ばれています。代表的な手法として Z、Bメソッド、VDM、SPIN、UPPAAL などがあります。

形式手法を利用すると、曖昧さのない厳密な設計や、設計が求められる性質を満たすかどうかの検証を行うのに役立ちます。最近ではモデル検査技術などコンピュータを利用した設計や検証の支援環境が整備されてきたことから産業界での利用が増えてきています。

特に自動車など高い安全性が求められるシステムでは機能安全規格 IEC61508、ISO26262 等への対応の際に、形式手法の利用が要求されるケースも生じています。



開発の課題

- ・高機能、複雑化
- ・安全性、信頼性
- ・短納期

形式手法を利用した設計及び検証

利用上の課題

形式手法を利用する場合、基本的には

- 仕様や設計を抽象化し、抽象モデルを生成する
- 抽象モデルを検証する

という作業を行います。しかし、利用してみると

- 数多くの手法の中から何をどのように利用すれば良いかわからない
- 自動化されていない、ツール間の連携が不十分であり、特定用途に対応していない

など、様々な課題が見つかり、利用の妨げになっている場合があります。

組込みシステム形式手法研究会

本研究会について

以上の背景及び課題から本研究会では、組込みソフトウェアおよび組込みシステムを主な対象とし、形式手法による設計及び検証の経験について情報交換を行っています。そして、利用上の知見や技術的な課題を整理します。今後、研究会の成果を公開することで産業界の技術向上に資することを目指しています。

研究会の活動状況

昨年度は Alloy、Event-B、プログラム検証ツール (BLAST, SDV など) などの手法やツールの調査及び試行を行い、利用方法などについての情報交換を行いました。

今年度も名古屋大学を中心とした各参加組織の会議室を利用し、およそ2ヶ月に一度の割合で開催しています。ご興味のある方はご連絡ください。

連絡先: 名古屋市工業研究所 電子情報部 齊藤直希
E-mail: saito.naoki@nmiri.city.nagoya.jp

謝辞

本研究会は(財)名古屋産業科学研究所の研究会として実施しています。名古屋産業科学研究所の皆様に感謝します。

