

Title	モデル検査手法1の普及に関する取り組み
Author(s)	青木, 利晃
Citation	
Issue Date	2007-09-06
Type	Presentation
Text version	publisher
URL	http://hdl.handle.net/10119/8257
Rights	
Description	北陸先端科学技術大学院大学 21世紀COEシンポジウム 「検証進化可能電子社会」 = JAIST 21st Century COE Symposium “Verifiable and Evolvable e-Society”, 開催：2007年9月6日～7日，開催場所：キャンパス・イ ノベーションセンター東京 国際会議室(1F)，2007年 9月6日（木），「JAIST-COE/AIST-CVS シンポジウム ：形式検証技術 現状と安心電子社会への適用」発表 資料

モデル検査手法の普及に関する取り組み

青木利晃

北陸先端科学技術大学院大学

安心電子社会研究センター

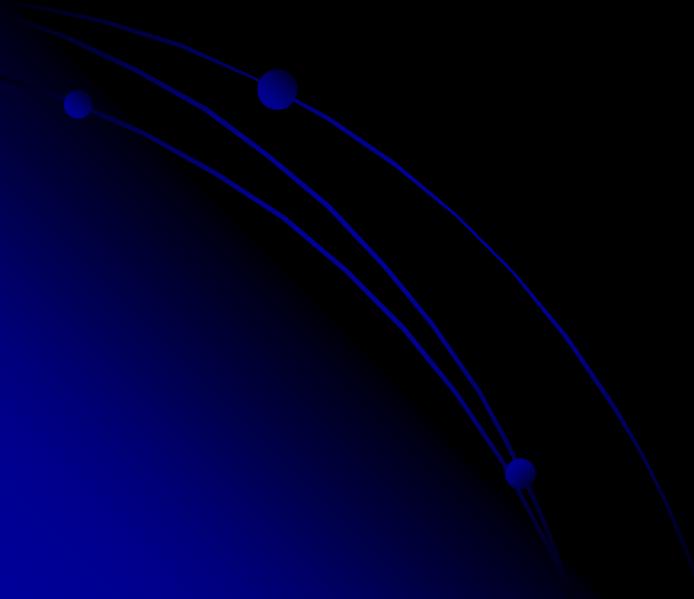
背景

- 形式手法への期待。
 - 信頼性低下に関する危機感。
 - 信頼性保証のためのコストの増大。
 - 経済産業省「情報システム信頼性向上に関するガイドライン」
 - 標準: 機能安全(IEC61508), セキュリティ(ISO/IEC15408)
- よく見えない形式手法の全貌。
 - とても広い分野なので見えにくい。
 - これが「形式手法」というものはない。
- 大学の役割。
 - 教育・研究機関。
 - 社会への貢献(正しい情報を提供する)。
 - 情報分野の実問題を解決する。

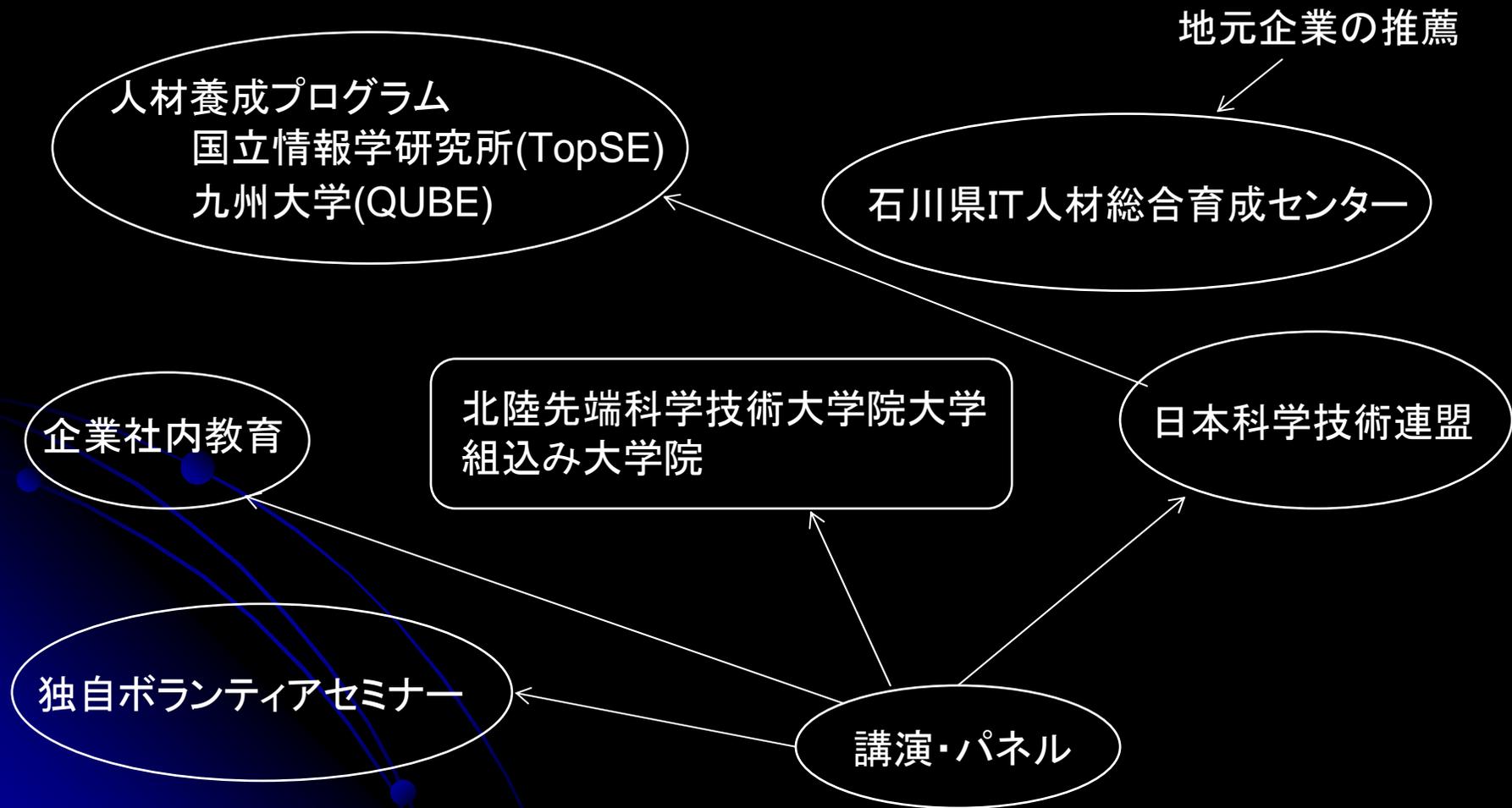
アプローチ

- 形式手法を正しく理解するためには？
 - キーワードだけでなく、技術の中身の理解。
 - 体験してもらうのが一番。
 - 形式手法理解の入り口としてのモデル検査手法。
 - 多くの前提知識を必要としない。
 - 簡便なツールが存在する。
 - 注目されている組込み分野で有効。
 - 限界がある→ほかの手法に興味湧く。
- 情報分野の実問題を解決するには？
 - 企業から問題の詳細を出してもらう。
 - すぐには難しい。失敗。
 - 企業内に形式手法を理解している人をつくる。
 - メリットは、最終的には、大学にかえってくる(共同研究など)。はず。。。

目的

- 形式手法の正しい理解を普及させる。
 - 情報分野の実問題を解決するための手段。
 - 組込み大学院への勧誘。
 - 他機関との連携促進。
- 

活動の概要



活動紹介

- 予備実験
 - 4回(2004~2005)
 - 対象:内輪(相談を受けた人にこっそり打診)
 - 状態遷移モデルとモデル検査(Promela/Spin)
 - 定理証明(HOL)とソフトウェア検証(Floyd/Hoare/Dijkstra)
 - 参加人数:約30名
 - 感触。
 - モデル検査は比較的うけがよかった。
 - モデル検査の概要を知っている人は、定理証明とソフトウェア検証の仕組みや原理を理解できていた。
 - 1日のセミナーなので、システムを使えるようにはならなかった。

活動紹介

- セミナー開催
 - 石川県IT人材総合育成センター(2004~2005)
 - 年2回開催
 - 内容
 - 状態遷移モデルとモデル検査(Promela/Spin)
 - 9:00~17:00×2日間
 - 参加人数:約20名
 - JAIST+日本科学技術連盟(2006~)
 - 年2回開催。
 - 内容
 - 状態遷移モデルとモデル検査(Promela/Spin)
 - 9:00~17:00×3日間
 - 参加人数:40名
 - JAISTと日本科学技術連盟の包括的な協定(日刊工業新聞2006年11月10日)

活動紹介

- 人材養成プログラムへの協力。
 - 九州大学QUBE(2006～)
 - モデル検査手法入門 –状態遷移モデルとモデル検査–
 - 年1回、9:00～17:00×2日間
 - 6名
 - 国立情報学研究所TOPSE(今年度から)
 - 設計モデル検査(基礎編)
 - 教科書執筆中。
- 個別企業における社内教育。

活動紹介

- JAIST組み込み大学院
 - 参加者: 15名(全員企業人、1/3が科目等履修生)
 - 90分×16コマ
 - 内容
 - 状態遷移モデルとモデル検査(Spin/Promela)
 - 形式体系と定理証明(HOL)
 - プログラム検証(Floyd/Hoare)
 - プログラム意味論(最弱事前条件)とプログラム導出(Dijkstra)

教授内容

- 状態遷移モデルとモデル検査(Spin/Promela)
 - 状態遷移モデルと振る舞い記述。
 - 振る舞いの特徴(非決定性と並行性)。
 - モデル検査の仕組みとSpin/Promela。
 - Promelaの書き方。
 - 様々な性質の検証(表明、デッドロック、進行性、性質オートマトン、LTL)。
 - マルチタスクソフトウェアへの応用。
 - 排他制御(交互実行/Dekker/Peterson)
 - 資源管理(Mutex/Semaphoreを用いた固定長バッファ問題 Reader/Writer問題の解決)
 - スケジューリング(sleep/wakeup, 優先度の取り扱い)
 - 組み合わせ問題の解き方
 - パズル的な問題(船頭・ライツアウト・ナイト交換など)

教授内容の特徴

- 独自作成の資料を配布する。
- 半日かけて状態遷移モデルの特徴について教える。
 - 状態遷移図で書いて検証するのが目的ではない。
 - 基本に加えて、並行性、非決定性、協調動作。
 - それぞれの振舞いをフラットな状態遷移モデルに展開させる。
 - それぞれの動作の解析の困難さや特徴が理解できる。

教授内容の特徴

- Spinを用いる理由。
 - RTOSのタスクや、システムプログラミングにおけるプロセスなどの概念に近い。
 - Promelaの記法がC言語などの手続き型言語に似ている。
- 最初の部分でも、純粋なTOYではなく、実際のシステムにおいて意味のある例を用いて解説する。
 - 排他制御、ロックなど。
- 並行プロセスやプロトコルの典型的な問題を事例として説明する。
 - 状態遷移図のような設計検証では、検証を行うまで様々な問題があり、応用法を理解しづらい。
 - 直接的に取り扱える事例を対象とすることにより、まずは、応用法の王道を理解する。
 - タネンバウムのOSの教科書内のサンプルプログラムを検証。
 - Dekker, Peterson, 生産者-消費者, Reader-Writer, ABP, etc.

教授内容の特徴

- 演習を細かく入れる。
 - 演習するだけでなく、それまでの資料を見直して理解できる。
 - 演習ができなくても、理解度が上がっている。
- 多くのサンプルを解説する。
 - わからないサンプルがあっても、他のものを見ているうちに理解できる場合が多い。
 - 90弱のサンプル。のべ4000行弱。

受講者について

- 幅広い参加者。
 - 大学教員、学生、工業試験場職員、新人（プログラミング経験なし）、ベテランエンジニアから管理職まで参加。
 - プログラミング経験なしの人もある程度は理解していた。
 - 改造、サンプルを見ながら記述することはできる。
 - 言語要素が少ないため、理解が容易？
 - 進み方や理解度にばらつきはあるものの、まったく理解できていない人はいない。
 - 使えるかどうかは別にして、モデル検査手法という技術がどのようなものかは理解できている。
 - 検証能力に驚く人と、導入はむずかしいと思う人に二分化。
→ 技術を正しく理解できているのでは？

感想について

- 受講者の感想（記憶している範囲）
 - 2/3くらいの参加者は使えると判断。
 - 時間が少ない。
 - アドホックな使い方はできそう。
 - 今の開発スタイルにどのように導入するかは難しい。
 - 現在携わっている開発とは関係なさそう。
 - 実開発の障害に適用した結果、2日ほどで解決できた。
 - 基本は理解したから、どのように実開発に適用するか教えてほしい。
 - 実際の適用事例について教えてほしい。

まとめ

- モデル検査手法の普及活動について紹介した。
- 2日間以上のセミナー・講義に参加した人数は100名を超えた。
 - そろそろ「入門編」としては頭打ちか？
 - 頭打ちになるまで継続する予定。
- 次のステップを準備。
 - モデル検査(応用編)
 - マルチタスクソフトウェアの検証。
 - ソフトウェア検証論
 - プログラム検証原理、定理証明手法。
- 個人レベルの活動ではなく、より広い枠組みを模索中。
- 企業へ戻った後のフォローアップの仕組み。

今後のスケジュール

- 2007年10/9～10
 - 九州大学人材養成プログラムQUBE
 - モデル検査手法入門 ー状態遷移モデルとモデル検査ー
- 2007年12月～毎週金曜
 - 国立情報学研究所人材養成プログラムTopSE
 - 設計モデル検査(基礎編)
- 2007年12/10-12
 - JAIST-日本科学技術連盟セミナー
 - モデル検査入門
- 2008年2月中旬～毎週土日
 - 北陸先端科学技術大学院大学 組込み大学院
 - ソフトウェア検証手法