Research Center for
Verification and Semantics

産業技術総合研究所
システム検証研究センター
News Letter
8
2007.11

プロジェクタでコラボ

初めてオーバーヘッドプロジェクタ、OHP なるものを見たのは高等学校の生物の授業においてだったと思う。まだ DNA のことが教科書に載っていなかったその頃、生物の先生が、板書の代わりにシートに内容を書いていかれたのが珍しかった。OHP の出現前にも、特に医学方面などで、35mm フィルムのスライドで投影しながら講演することもあったようだが、知らなかった。

さて、大学を出てアメリカの会社に勤めてみたら、ちょっとした会議にでも、どんどん OHP を使うのに驚いた。シートを沢山使うが、一枚一枚は、高等学校でみたものより薄く粗末なものだった。会社から大学院に舞い戻った後も、研究会で話すのにやはり OHP を使った。講演の要点を予め記しておき、これを見せながら話すことによって、講演の進め方が変わったように思う。

時代は変って、コンピュータから送られる画像を投影する、所謂プロジェクタに OHP はとって代わられた。OHP にしろ、プロジェクタ用のスライドデータにしろ、講演の直前まで修正できる機動性が講演者にとっての魅力である。そのせいで、スライドを印字して事前に聴衆に配るのは難しくなった。尤も、スライドを印字したものがどの程度有用なのかは疑問だ。予稿がある場合には屋上屋を架すことになるだろう。文章ではなく単語の羅列であるスライドを流通させる事には、正確な情報を流通させる観点からは問題があるかもしれない。最近は、講演後にスライドデータを集めて WEB に張り出す場合も多い。コンピュータのファイルだから集められるので、OHP では集めるのも大変だったろう。

講演などの発表用だけではなく、編集用にプロジェクタを使うことも多くなった。共同で文章を書くのに、プロジェクタは有効である。一人が書いた草稿に他のものが朱を入れる事を繰り返すのが、共著で文章を書くときの普通の方法だったように思われる。プロジェクタを使うやり方では、テキストエディタの画面をプロジェクタで映し出し、一人が文章を入力していく。他のものはそれを見ながら語句の修正を指摘する。入力者以外のものが文を口述する場合もある。こうして出来上がる文章は、その場にいるもの全員による共著の文章というに相応しいものである。無線接続のキーボードとマウスの御蔭で、会議室の大きなテーブルのどこに座っても、キーボードとマウスを使うことができる。他に必要なものはスクリーンか。しかし映像は壁に映してもよいのだ。

2007 年 11 月　　センター長　木下佳樹

＜CVS ニュースレター　8 号＞

産業技術総合研究所　システム検証研究センター http://unit.aist.go.jp/cvs/
●千里サイト　：〒 560-0083　大阪府豊中市新千里西町 1-2-14　三井住友海上千里ビル 5F
●関西センター：〒 563-8577　大阪府池田市緑丘 1-8-31

●トピックス１

JST「情報社会を支える新しい高性能情報処理技術」第４回領域シンポジウム参加報告

システム検証研究センターは、さる 2007 年 10 月 12 日に、科学技術振興機構 (JST) の主催で行われた戦略的創造研究推進事業 (CREST) 研究領域「情報社会を支える新しい高性能情報処理技術」の第 4 回領域シンポジウムに参加し，木下センター長による講演と、ポスター展示発表を行いました。

この研究領域は、情報セキュリティ大学院大学研究科長の田中英彦教授が研究総括で、従来のコンピュータシステムを新たな時代の要求に合わせて変革するための要素技術を対象として、11 のプロジェクトで研究が行われてきました。システム検証研究センターは、2002 年より参加して、「検証における記述量爆発問題の構造変換による解決」というプロジェクトを遂行してきました。本年度が 5 年目で、最終年度にあたります。

今回、東京の日本科学未来館で行われた領域シンポジウムには、7 プロジェクトが参加しました。当センターの発表内容をご報告します。

システム検証研究センター　田辺 良則

◆発表概要

このプロジェクトの目的は、抽象化と呼ばれる手法によって、膨大な記述量を持つシステムの検証を可能にし、ソフトウェアの信頼性を抜本的に向上させることにありました。研究成果は、以下の３つのグループに分けられます。

最初は、抽象化理論です。様相 μ 計算の部分系 R μ を構築し、抽象化シナリオの数理モデルを研究しました。これは、木下 -Power による、入力出力型システムに関する理論を刺激応答系に具体化したものと考えられます。また、命題様相 μ 計算を自然に拡張した一階様相 μ 計算の研究も行い、その基礎理論を確立しました。

第 2 に、抽象化支援ツール MLAT の試作構築を行いました。ポインタで作られたデータ構造を扱うプログラムの抽象化は、単純なデータの場合とは違った困難があります。MLAT は、様相論理を利用した抽象化を行うことによって、この困難を克服しようとするツールです。数回にわたる論理の拡張を行った結果、DSW という算法の正当性検証に成功しました。

第 3 は、統合検証環境 Agda-IVE の構築と、実問題への適用です。Agda は、Chalmers 工科大学で開発が始められ、当センターも開発に加わっている対話型証明支援系です。統合環境 Agda-IVE では、モデル検査器 SMV、 一階述語論理自動証明器 Gandalf、 抽象化支援ツール MLAT などの外部ツールを Agda から呼び出し、またその結果を Agda に取り込むことができます。実問題への適用可能性を調べるため、YAMPII という並列計算用ライブラリの、通信要求を管理する部分を取り上げました。約一ヶ月をかけて正当性の検証を行うことができました。

このプロジェクトをきっかけとして設置された当研究センターの活動が、国内のこの分野の技術移転に先導的役割を果たしてきました。基礎研究を今後も発展させるとともに、企業と連携した実用研究との融合を推進することで、日本の情報技術の本格的な進展に寄与したいと思います。

JST 第 4 回領域シンポジウム参加者

ポスターセッション

産業技術総合研究所　システム検証研究センター http://unit.aist.go.jp/cvs/
●千里サイト　：〒 560-0083　大阪府豊中市新千里西町 1-2-14　三井住友海上千里ビル 5F
●関西センター：〒 563-8577　大阪府池田市緑丘 1-8-31

●トピックス２

「第四回システム検証の科学技術シンポジウム」開催報告

11月5日(月)～11月7日(水)の日程で、名古屋大学野依記念学術交流館において開催されました。今年度からは日本ソフトウェア科学会ディペンダブルシステム研究会の主催で行われ、システム検証研究センターは共催いたしました。

システム検証の科学技術に関する以下のようなテーマで、招待講演、一般講演、デモ・ポスター発表を３日間にわたり合計35件行いました。今回のシンポジウムには９４名参加していただきました。その内訳は３６名が産業界から、３３名が大学から、２５名が大学以外の公的機関から、とバランスの取れた分布になりました。産業界と学界にまたがった研究交流の場を提供することができたのではないかと思います。

・ディペンダビリティ・機能安全・セキュリティ・生産性
・数理的技法（formal methods）・モデル検査・定理証明
・プログラミング意味論・書換系・テスト技法・品質保証
・ソフトウェア開発方法論・検証手法の導入研究

１１月５日（月）

会場の野依ホールは非常にすばらしい会場でした。改めて名古屋大学の協力に感謝します。その名古屋大学から、大学院情報科学研究科長の古賀伸明先生から開会の挨拶を頂きました。招待講演の石川先生は、ソースコードレベルの検証の重要性を熱心に訴えられ、検証技術への期待を述べられていました。

・・・・・・・・　１日目プログラム　・・・・・・・・

●招待講演
「システムソフトウェアにおける検証技術への期待」　石川　裕（東京大学大学院）
●一般講演
「プロセス計算による定性的コスト解析とネットワークシミュレータによるコストの定量的コスト解析」　池田立野、西崎真也（東京工業大学）
「An Algorithm for Bounded Multi-Valued Model Checking」　Jefferson O. Andrade, Yukiyoshi Kameyama（University of Tsukuba）
「リアクティブシステム仕様の強充足可能性判定問題の計算量について」　島川昌也、萩原茂樹、米崎直樹（東京工業大学）
●システム検証研究センター研究紹介
「機能安全のためのソフトウェア認証制度普及に向けた取り組みの紹介」　長谷部浩二（産業技術総合研究所）
「研修コース研究開発」　西原秀明（産業技術総合研究所）
「MLAT」　田辺良則（産業技術総合研究所）
「Agda IVE の実用問題への適用」　加藤紀夫（産業技術総合研究所）
「図示記法」　吉田　聡（産業技術総合研究所）、小池憲史（矢崎総業株式会社）、竹内　泉、大崎人士（産業技術総合研究所）
「業務システム開発検証ツール」　髙木　理（産業技術総合研究所）

１１月６日（火）

この日の参加者が最も多く活発な議論が行われました。デモ・ポスターセッションを午後に設けていましたが、発表が７件に増えたため、４０分間では十分な議論ができなかったことが残念でした。今後の改善点にしたいと思います。高浜先生の招待講演では、興味をかきたてられる飛行制御システムの例を交え、制御の信頼性に関する議論が非常に楽しく行われました。この日は最後に林先生の招待講演が行われました。システムというと機械などの装置を思い浮かべがちですが、社会システムなど人間を含んだ大きなシステムもあるということに気づかせてもらいました。これらシステムの検証技術の必要性を考えさせられました。夕方に懇親会が行われました。シンポジウムの参加者の半数以上が懇親会にも参加されたことが特徴的でした。懇親会ではリラックスした雰囲気で自由に意見交換が行われ、参加者どうしの非常によい交流の

◆シリーズコラム

機能安全（第２回）「機能安全の方法」

連載第２回目の今回は、前回紹介した機能安全規格 IEC 61508 が、機能安全を達成するための方法として、ソフトウェア開発に求めている要求事項についてまとめてみたい。

E/E/PE 安全関連系では、ハードウェアのみならず、ソフトウェアに対しても、相応の「安全性」が求められる。ソフトウェアは、求められる安全機能（制御対象の安全状態を確保する機能や、ハードウェアおよびソフトウェア自身の異常検出機能等）を、求められる水準で確実に実行できなければならない。そのためには、ソフトウェアの設計・開発において、安全性に関する要求仕様を正しく獲得することと、それを正しく高信頼に実現することが必要となる。

こうした作業において生じる間違いがソフトウェアのバグであり、IEC 61508 では決定論的原因故障として分類している。決定論的原因故障については、ランダムハードウェア故障とは異なり、発生確率に基づく評価や対策ができない。そこで IEC 61508 では、ソフトウェアのバグを回避もしくはマネージすることを目的として、ソフトウェアの開発プロセスに関する要求事項を規定しており、それが満足されることによって機能安全が達成されるというアプローチを取っている。

IEC 61508 第３部で規定される開発プロセスは、「ソフトウェア安全ライフサイクル」と呼ばれる。なおこれは、先立つ第１部において安全関連系全体に対する開発・運用プロセスとして規定される「全安全ライフサイクル」の一部である。ソフトウェア安全ライフサイクルは、伝統的な V 字モデルの開発プロセスを含むものであるが、以下の特徴は注意が必要であろう。

•各工程において使用が推奨される手法や技

産業技術総合研究所　システム検証研究センター http://unit.aist.go.jp/cvs/
●千里サイト　：〒560-0083　大阪府豊中市新千里西町 1-2-14　三井住友海上千里ビル 5F
●関西センター：〒563-8577　大阪府池田市緑丘 1-8-31

場になったと思います。

● ● ● ● ● ● ● ● 2日目プログラム ● ● ● ● ● ● ● ●

●招待講演
「制御システムにおける制御性能の限界と信頼性の関わり」
高浜盛雄（名古屋大学大学院）
●一般講演
「ソフトウェア製品の不具合原因となるコードのパターンを用いた検証手法」
福原和也、猪股俊光、新井義和、曽我正和（岩手県立大学）
「ソフトウェアシステムの構成変更における Alloy を用いた整合性検証」
谷崎裕明、片山卓也（北陸先端科学技術大学院大学）
「モデルベース開発における自動化フレームワーク」
黒岩正司（富士設備工業株式会社）
「環境ドライバを用いたモデル検査による検証事例」
高井利憲（産業技術総合研究所）、古橋隆宏（矢崎総業株式会社）
尾崎弘幸、大崎人士（産業技術総合研究所）
「システム検証の事例報告集の作成」
渡邊　宏、奥野康二、高井利憲（産業技術総合研究所）
●デモ・ポスター発表
「モデル検査支援ソフトウェア」
篠崎孝一（関西電力株式会社）
早水公二（メルコ・パワー・システムズ株式会社）
「FODA フィーチャーダイアグラムの自動検査法」
中島　震（国立情報学研究所）、鵜林尚靖（九州工業大学）
「プロダクトライン開発の延長上にある、専用のモデル環境」
浅野義雄（富士設備工業株式会社）
「統合検証環境 Agda-IVE」　湯浅能史、武山　誠（産業技術総合研究所）
「プロダクトライン開発のための設計検証ツール」
野田夏子（日本電気株式会社）
岸　知二（北陸先端科学技術大学院大学）
「通信プロセスモデルに基づく AIBO OPEN-R プログラムの並行オブジェクトの同期フロー解析」　末次　亮、結縁祥治、阿草清滋（名古屋大学）
「セッション型の実装に基づく検証可能なネットワークプログラミング」
今井敬吾、結縁祥治、阿草清滋（名古屋大学）
●一般講演
「Real-Time Maude によるモデル検査事例と検査式およびモデルの修正方法」
中野昌弘、高井利憲（産業技術総合研究所）
「オーバーラップ制御の設計と検証」　藤倉俊幸（イーソル株式会社）
「アセンブラプログラムのモデル検査によるバグ解析事例」
吉田　聡、高井利憲（産業技術総合研究所）
●招待講演
「危機対応業務の標準化を目指した業務の見える化手法 BFD の開発」
林　春男（京都大学）
●懇親会

11月7日（水）

アイシン精機の鈴村様の招待講演では、車載ソフトウェアに関する国際的な活動に関して詳しく聞くことができました。学会が夏に函館で行っているワークショップのなかから、二件の講演がセレクトされて再発表されました。ワークショップは学術的な面が中心ですが、その活動を産業界の人にも感じてもらえたらよいと思います。また逆に、今回のシンポジウムで発表された事例研究のいくつかを次回のワークショップで再発表し、産学の交流を深めていきたいと考えています。

大きなトラブルもなく、無事シンポジウムを終わらせることができたことに、関係者および参加者に深く感謝します。

副センター長　高橋 孝一

● ● ● ● ● ● ● ● 3日目プログラム ● ● ● ● ● ● ● ●

●招待講演
「車載ソフトウェア標準化プラットフォーム AUTOSAR と底流に見られる欧米の産学官連携活動」
鈴村延保（アイシン精機株式会社）
●一般講演
「モデル検査器を使った船舶用システムの検証について」
八尾俊祐、高橋和子（関西学院大学大学院）
粟野宏昭、平岡　康（古野電気株式会社）
「モデル検査活用のための実践的知識」
篠崎孝一（関西電力株式会社）
早水公二（メルコ・パワー・システムズ株式会社）
●函館ワークショップ特別講演
「エラー情報から原因を特定する障害検知システム」
酒井将人、松葉浩也、石川　裕（東京大学大学院）
「Comparison of the Expressive Power of Language-based Access Control Models」
関　浩之（奈良先端科学技術大学院大学）、高田喜朗（高知工科大学）
●一般講演
「n 点通過テストのためのモデル検査技法」
小池憲史（矢崎総業株式会社）、大崎人士（産業技術総合研究所）
「構文からみた時相論理で記述されたリアクティブシステム仕様の性質について」
吉浦紀晃（埼玉大学大学院）
「記号モデル検査による自己安定アルゴリズムの安定時間の計測」
木本雅博、土屋達弘、菊野　亨（大阪大学大学院）

● ● ● ● ●

法を、安全度水準に応じて規定している。

- 安全要求仕様としてソフトウェアが実現すべき安全機能と、その安全度水準の明記を求めている。
- 設計の各工程に対する適合確認（verification）および妥当性確認（validation）の計画的な実施を求めている。
- ソフトウェア修正についても手順を規定している。

これらに加えて、全工程を通じた、文書化、ソフトウェア品質管理および機能安全評価の実施が求められている点にも注意されたい。文書化は、関連業務の効果的な実施のために、必要な情報の文書化と管理を求めるものである。ソフトウェア品質管理は、ソフトウェア安全ライフサイクルの実施における管理業務の明記を求めるものである。考慮すべき項目として、機能安全達成の戦略、各工程の担当者と担当組織、是正勧告等への対処方法、構成管理の手順、作業担当者の適正等が挙げられている。また、機能安全評価は、安全関連ソフトウェアによって目標とする機能安全が達成されたかどうかを判定する作業であり、結論として合格、条件付合格、不合格のどれかを勧告するものである。評価者には、安全度水準に応じた独立性が求められている。

以上のように、IEC 61508 では安全関連ソフトウェアに対する技術的要求事項として開発ライフサイクルを規定するものであるが、管理や評価等の非技術的要求事項も合わせて規定することで、いわば安全な組織による確実な安全達成を求めていると言える。もっとも、ソフトウェア安全ライフサイクルはあくまでも全安全ライフサイクルの一部であり、最終的にソフトウェアがシステムレベルの安全にどう貢献するかという視点が常に必要である。実際、規格の第 3 部は、第 1 部および第 2 部を適宜参照していることに触れておく。

システム検証研究センター　水口 大知

産業技術総合研究所　システム検証研究センター http://unit.aist.go.jp/cvs/
●千里サイト　：〒 560-0083　大阪府豊中市新千里西町 1-2-14　三井住友海上千里ビル 5F
●関西センター：〒 563-8577　大阪府池田市緑丘 1-8-31

● CVS ニュース

イリノイ大学から活動報告 vol. 1

当研究センターの大崎 人士主任研究員が、2007 年 6 月よりイリノイ大学において在外研究を行っています。その活動について 2 回にわたって報告します。

■大崎レクチャー

イリノイ大学（University of Illinois at Urbana-Champaign, UIUC）での在外研究をスタートしてすぐに、専門分野に関する講義資料の作成を行いました。全十回からなるこの講義は、一回二時間の内容で、形式言語、計算可能性や計算量、半線形集合と線形代数、ツリーオートマトンとその応用に話題が及びます。Jose Meseguer 教授（受入ホスト）からは、ようやく完成した講義を試験的に講演する機会をいただきました。また、イリノイ大学日本人会の関連研究者ら向けにも、大崎レクチャーの名称で、話題を選んで講演しています。

■自分の時間

イリノイ大学（UIUC）には、研究内容に接点のある研究者が多く、実際の研究活動の中で議論を交わしたり、セミナーで話したりする機会を多く持つことができます。こうした経験の中で、「自分の時間は自分のもの、という考え方を尊重する雰囲気」を学びました。例えば，セミナーとはいえ、話につきあうかどうかは、そのとき自分で決める事をよしとしています。したがって、話す方も、なぜその話をするのか、聞き手が分からなくなっていないか、に注意を払う機会が増えます。講演や討論のコツというよりは、こちらの考え方と、今までの自分のやり方を照らし合わせる良い機会を得たと感じています。

■日本人的考え方

いっぽうで、日本人的な考え方、というのも一つの見方としてよい基準になります。例えば、論文投稿の最終段階で、コメントを求められることがよくあります。主張を前面に押し出すような書き方に抵抗を感じたので、「論文の主張を、独善的でなく、いかに他の研究と調和させるかについて述べるべき」というコメントをすると、『目から鱗』のような反応をされることがあります。全体主義的な、調和を重んじる東洋的な考え方は、科学論文の書き方にも、違いを生じさせるのだと気づいた経験でした。

■古きもの

では、ものづくりの分野では、果たして「古い物は、新しい物に置き換えるべき」という発想が正しいのでしょうか。ものを作るのが器用、と言われている日本人は、実は、過去の遺産をないがしろにしなかったので、ものづくりを上手にできたのではないでしょうか。ものを作り続けるには、進んだ技術をいかに従来の技術と融合させるかを考えることが、結構大事なんだと思います。海外でウケる主張をするか、『大事なこと』を実行に移すか、悩み多きところです。

■ものづくり工学

ということは、ものづくりのあり方について述べようとするとき、それを論文にして、海外の会議に投稿して評価されなかったからといって、その論文の価値を判断するのは早計かもしれません。考え方の違いは、文化の違いという本質的な問題であることも多く、説得するのは至難の業です。そろそろ、日本発の「ものづくり工学」分野を、世界に向けて発信するべきなのではないでしょうか。

2007 年 11 月

システム検証研究センター　大崎 人士

イリノイ大学　計算機科学科棟

● ● ● ● ●

産業技術総合研究所　システム検証研究センター http://unit.aist.go.jp/cvs/
●千里サイト　：〒 560-0083　大阪府豊中市新千里西町 1-2-14　三井住友海上千里ビル 5F
●関西センター：〒 563-8577　大阪府池田市緑丘 1-8-31

●イベント・講演会

2007 年 10 月～ 2007 年 12 月
イベント開催報告

◆計算機言語談話会（CLC） 原則毎週木曜日 定期開催中

日付	講演者（所属）
10/29	Farn Wang（National Taiwan University）
11/15	関澤 俊弦（CVS）

【開催場所：システム検証研究センター千里サイト】

直近のスケジュールはこちらから▼
CLC の URL：http://unit.aist.go.jp/cvs/CLC/

◆システム設計検証技術研究会 2 ヶ月毎に開催中
（産総研コンソーシアム）

第四回　2007 年 11 月 22 日 木　開催

講演者　徳岡 宏樹氏（日本電気株式会社ソフトウェアエンジニアリング本部）

演　題　「C 言語ソースコード検証へのモデル検査法の適用」

概　要　社会システム・工業製品のソフトウェアへの依存が高まる中、ソフトウェアの安全性・信頼性のより一層の確保が求められている。特に、組込み領域ではソフトウェア開発規模の飛躍的な増加に伴い、効率的な品質の確保が大きな課題となっており、その解決に向けて形式手法が注目されている。本発表では、形式手法の一種である有界モデル検査法を応用して、C 言語のソースコードから実行時エラーを検出するツールに関して、その社内適用で得た、不具合検出などの実績と運用上の課題などを報告する。

第五回　2007 年 12 月 17 日 月　開催

講演者　田正司 昌則氏（メルコ・パワー・システムズ株式会社）
大西 康夫氏（日本コンピュウェア株式会社）

演　題　「継続的な品質の”見える化”とツール適用の実際」

概　要　前半は、ツール利用者の立場から、現場にツールを定着させるための取り組を紹介する。高価なツールを購入しても現場で活用されず眠っているという事例は枚挙に暇がない。実案件を通してツールの効果を確認した事例を紹介し、ツールが活用されない原因がどこにあるのか、開発者に負担をかけずに短時間で成果を上げるためには何が必要か、現場の技術者の視点で調査したことで見えてきた問題点と、それを解決するために行った現場主体のカイゼン活動を紹介する。後半はテストソリューションベンダー側からの視点で発表する。システム開発成功のためには、開発の各フェーズで継続的に品質を”見える化”すなわちツールによる分析を行い、早い段階で欠陥を除去することが有効である。開発の各フェーズである要件定義から運用においてツールを使用した品質の可視化について現場での適用例を示すとともに、アメリカにおける最近の技術動向を紹介する。また画面オペレーションやチェックなどの自動化による機能テスト自動化手法なども紹介する。

【開催場所：システム検証研究センター千里サイト】

直近のスケジュールはこちらから▼
コンソーシアムの URL：http://unit.aist.go.jp/cvs/consortium/

システム設計検証技術研究会とは

本研究会の会員に対して、数理的技法に基づく検証法についての講演、さまざまな検証ツールの紹介など、分野の枠を超えた交流の機会を提供しています。

●募集時期：毎年 4 月以降に入会を受け付けています。

●年会費

1. 法人会員：10 万円（企業）

　＊ 1 企業で何名様でも講演会にご参加いただけます。

2. 個人会員：無料（大学、非営利団体に在籍の個人）

詳しくはこちら▼
URL:http://unit.aist.go.jp/cvs/consortium/

講演風景

出版

◆テクニカルレポート

10 月発行

PS-2007-010

Toshinori Takai, Takahiro Furuhashi, Hiroyuki Ozaki, Hitoshi Osaki
" 環境ドライバを用いたモデル検査による検証事例 "

※全てのテクニカルレポートは HP から入手可能です。

URL：http://unit.aist.go.jp/cvs/techrep.html

編集・発行：独立行政法人産業技術総合研究所
システム検証研究センター
連　絡　先：〒 560-0083
大阪府豊中市新千里西町 1-2-14
三井住友海上千里ビル 5F
Email：informatics-inquiry@aist.go.jp