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 9
2008.02

意味論について

システム検証研究センターの英語名は Research center for verification and semantics としている。Semantics の訳語にはふつう、意味論があてられる。この語を研究センターの日本語名にいれなかった理由はいくつかあるが、それはさておき、今回は、意味論について少し書いてみたい。

わが国の現状ではあまり広く知られていないように思われるからである。意味という言葉から、哲学的な考察が想像されるかもしれない。しかし、計算機科学で意味論と呼ぶのは、プログラムや情報処理過程の数理モデルを構築するための理論である。もともとはプログラミング言語の意味を確定させようとする試みに、言語学で使われていた semantics という語をあてたが、この英単語にはすでに意味論という訳語があてられていた、というところであろう。自然言語の意味を与えるのではなく、プログラムやプログラミングの意味論という意味で算譜意味論とかプログラミング意味論ということも多い。

「数理モデル」という言葉に説明が必要だろう。これは数学的な枠組を用いて情報処理システムを記述したものである。数学的な枠組とは、現代数学では集合と写像によって構成される世界であるといってよい。集合論あるいは圏論によってこのような世界の基盤が築かれている。その世界の中で情報処理システムを記述しようというのが意味論である。

さてそれでは、意味論がシステム検証にどう関わるのか。システム検証といっても、テストやレビュー、数理的技法などのいろいろな技法があるわけだが、とくに数理的技法において、モデル化の枠組を与えるのが意味論である、ということができる。数理的技法は、情報処理システムを数学的な対象としてモデル化し、それに望まれる性質が成り立つ、という命題を証明することによってシステムの動作の正当性を主張しようとする技法であった。その第一段階であるモデル化に必要な数学的対象の枠組を正確に規定するのが意味論である。システムをどのように記述するのか、という興味から意味論の研究を始めることができる。筆者もそのようにして意味論研究の世界にはいったのだが、システム検証の数理的技法の場を提供する実用的なものとして意味論を捉えることもできるのである。

意味論の数学的世界と現実のシステムをどのように関係付けるのかという問題がさらに発生する。語彙を提供するオントロジー、さらには現実の要求を調べるシステム分析などという技術がそれを受け持つ。

2008 年 2 月

センター長　木下佳樹

＜CVSニュースレター　9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

●活動紹介

計算機言語談話会（CLC）（Computer Language Colloquium）

今回は、計算機言語談話会 (CLC) をご紹介いたします。CLC は、システム検証研究センター (CVS) で、原則として毎週木曜日に行っている研究セミナーであり、当研究センターを含む国内外の研究者が講演を行っています。

■ CVS の共通知識基盤

今回ご紹介する CLC は、CVS の前身である電子技術総合研究所時代から、産総研の研究センターに発展した今日にいたるまで、継続して行なわれている研究セミナーであり、その研究活動の中心的な役割をになっています。もう一つの CVS の活動である「システム設計検証技術研究会」が、主として実用段階に近い検証技術の普及を目的にしているのに対し、CLC の講演内容は、より学術分野に重きをおいています。CVS にはいろいろなバックグラウンドを持った研究員が集まっているため、CLC を通して共通知識基盤の形成を図っています。CVS 研究員は、特別の事情がないかぎり CLC に出席するようにしています。

■多彩な講演

CVS 研究員の興味を反映して、ソフトウェアの基礎理論から技術の応用にいたるまで、さまざまなトピックの講演が行われています。もちろん、CVS 研究分野に関係の深い講演が中心ですが、ときには、必ずしも CVS の研究テーマに近いとは限らない講演もあります。例えば第 156 回には、東京大学の近山先生に、コンピュータ将棋ソフト「激指」とその関連技術についてお話を伺いました。計算機科学の成果がどのように将棋ソフトに反映されるか、また、逆に将棋ソフトを強くするための工夫が計算機科学にフィードバックされる様子など、興味深い内容に加え、「激指」開発初期のエピソードなどもお話しいただけました。また、CVS に長期滞在される研究者の方に、連続講義を行っていただくこともあります。最近では、第 182-184、190、191 回に、シャルマース工科大学の Bengt Nordström 教授に、構成的型理論について講義をしていただきました。

■ご聴講を歓迎します

CLC は、全講演を公開で行っております。ここで講演される研究に興味をお持ちの方でしたら、どなたでも気軽に参加いただけます。もちろん聴講は無料ですし、事前に参加申込をする必要もありません。会場は、大阪府豊中市にある CVS の千里サイトの会議室です。リラックスした雰囲気のなか自由な議論が交わされ、様々な人や研究が邂逅し、新たな研究が自然発生的に生まれる場となっています。

講演予定をご案内するメーリングリストを用意しております。配信を希望される方は、CLC 事務局 (clc-staff@m.aist.go.jp) あてにご連絡ください。また、http://unit.aist.go.jp/cvs/CLC/ で、講演予定と過去の講演の梗概をご覧いただけます。

【平成 19 年度実施　CLC 講演会一覧】

196 回（4/5）	松本　眞氏（広島大学）
197 回（4/12）	Armin Lawi 氏 (九州工業大学)
198 回（4/19）	鹿島　亮氏 (東京工業大学)
199 回（5/10）	竹内　泉 (CVS)
200 回（5/10）	吉田　聡 (CVS)
201 回（5/31）	Michael Winter 氏 (Department of Computer Science, Brock University)
202 回（6/28）	長谷部浩二 (CVS)
203 回（7/5）	Li Xin 氏 (Japan Advanced Institute of Science and Technology)
204 回（7/12）	長谷部浩二 (CVS)
205 回（7/26）	高井利憲 (CVS)
206 回（7/31）	松岡　聡 (産総研 計測標準研究部門､システム検証研究センター)
207 回（9/25）	Jiri Adamek 氏 (Institute of Theoretical Computer Science,Technical University of Braunschweig, Germany)
208 回（10/4）	武山　誠 (CVS)
209 回（10/11）	吉田　聡 (CVS)
210 回（10/18）	田辺良則 (CVS)
211 回（10/18）	木下佳樹 (CVS)
212 回（10/25）	高木　理 (CVS)
213 回（10/29）	Farn Wang 氏 (National Taiwan University)
214 回（11/15）	関澤俊弦 (CVS)
215 回（12/18）	Jean-Pierre Jouannaud 氏（Laboratoire d'Infomatique, École Polytechnique）
216 回（1/31）	西村　進氏（京都大学大学院理学研究科）
217 回（2/14）	松野　裕氏（東北大学電気通信研究所）
218 回（2/21）	高村博紀 (CVS)

2007 年度研究プロジェクト報告会のご案内

実施したプロジェクトごとに担当研究者による発表を行います。

日時：2008 年 3 月 13 日（木）13:30 ～ 16:30（参加費無料）
場所：産業技術総合研究所関西センター融合棟2F　多目的ホール
主催：システム検証研究センター
詳細は、http://unit.aist.go.jp/cvs/topics/topics9-Prj3-080130.html
聴講申込み、お問合せは、cvs-project-fy2007@m.aist.go.jp まで。

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

●会員募集

産総研コンソーシアム
システム設計検証技術研究会
平成 20 年度会員募集

システム検証研究センターでは、システム設計および開発に資する検証技術の普及を活動目的として、産総研コンソーシアム・システム設計検証技術研究会を開催しています。ここでは、数理的技法に基づく検証技術についての講演や、世の中で広く使われている検証ツールの紹介を行っています。

■平成 19（2007）年度活動内容

本研究会は会員制で、平成 19 年度会員数は組織は 14 団体、個人は 6 名でした。本年度は、講演会を中心に活動しました。主に国内の大学や企業から講師をお招きし、全 7 回の講演会を開催いたしました。

※講演内容は速記録としてまとめられ、会員限定で配布しております。

各講演会の後は、講師を囲んで、講演中にできなかった質問や普段では聞けない苦労話から、この分野のトレンドにいたるまで様々なお話ができる交流の場を提供しております。会員の皆様には講演とともに、交流会も収穫の多い場となっています。

■平成 20 年度会員募集

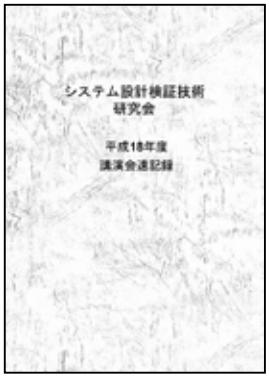
現在、平成 20 年度の会員を募集しています。本研究会は会員制です。法人会員（企業）と個人会員（大学、非営利団体に在籍する個人）がありますが、いずれも産総研（AIST）の承認が必要です。システム設計検証技術研究会の会員は、システム検証研究センターが主催する講演会やその他イベントへ優先的に参加することができます。また速記録も配布されます。

年会費：

法人会員　10 万円　　個人会員　無料

注 1）法人会員は 1 企業で何名様でも講演会にご参加いただけます。
注 2）企業在籍の方は法人会員としてのご参加をお願いします。

詳しいお申込み方法は、CVS/AIST のホームページ（URL:http://unit.aist.go.jp/cvs/conso-top.html）をご覧の上、事務局にメールにてお申込み下さい。



システム設計検証技術研究会
速記録

速記録には、講演で使用した発表資料とともに、講演内容だけでなく、質疑応答までも忠実に再現し掲載しております。レファレンスに最適な一冊です。平成 19 年度の速記録は、3 月下旬に発行予定です。

◆シリーズコラム

機能安全（最終回）
「機能安全の認証」

連載第 3 回目（最終回）の今回は、機能安全規格 IEC 61508 に対する適合認証の方法と現状について述べたい。

IEC 61508 に対する認証活動は、現在のところ欧州のいくつかの認証会社によって実施されており、適合性が認証された製品が既に市場に出ている。その主な例としては、センサ、コントローラ、ネットワーク通信機器などの安全計装系のためのコンポーネント機器がある。また、ソフトウェア単体でも、認証を取得したリアルタイム OS やコードジェネレータが存在する。

機能安全の認証に際して、認証機関では IEC 61508 が規定している機能安全評価と同等の作業を実施している。前回も述べたが、機能安全評価とは、全安全ライフサイクルの各フェーズにおける活動や成果物を詳細に検討して、規格の目的および要求事項が満たされているかどうか、そして、E/E/PE 安全関連系によって機能安全が達成されているかどうかの判定を下す作業である。開発側はこの評価作業を、外部の認証機関に依頼するのが一般的となっており、その判定結果が合格であれば認証証書が発行される。

機能安全評価への要求事項は、数は多くないものの重要で難しいものがほとんどである。例えば評価の範囲については、全安全ライフサイクルのすべてのフェーズと規定しており、適合確認（verification）、妥当性確認（validation）、監査等の結果を踏まえた総合的な判断を求めている。また評価実施者には、関係するすべての人、情報

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

平成 20 年度も、国内外から著名な講師を招聘し、産総研コンソーシアムとして有益な講演会を開催してまいります。活動内容に関しまして、皆様からのご意見ご要望がございましたら、事務局までメールにてご連絡ください。

今後とも、システム設計検証技術研究会の活動にご支援賜りますようお願い申し上げます。

平成 20 年 2 月

システム設計検証技術研究会　事務局

平成 19 年度総会

【平成 19 年度実施　産総研コンソーシアム講演会一覧】

第 1 回講演会（平成 19 年 7 月 20 日）
「Model Checking を適用した実践的非同期制御検証」
山本訓稔氏、服部彰宏氏（富士ゼロックス株式会社オフィスプロダクト事業本部コントローラーソフトウェア開発部）

第 2 回講演会（平成 19 年 9 月 27 日）
「組込みソフトウェアの高信頼化開発手法」
中本幸一氏（兵庫県立大学大学院教授、名古屋大学大学院情報科学研究科附属組込みシステム研究センター特任教授）

第 3 回講演会（平成 19 年 10 月 26 日）
「モバイル FeliCa IC チップ開発における形式仕様記述手法の導入」
栗田太郎氏（フェリカネットワークス株式会社 開発部）

第 4 回講演会（平成 19 年 11 月 22 日）
「C 言語ソースコード検証へのモデル検査法の適用」
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）

第 5 回講演会（平成 19 年 12 月 17 日）
「継続的な品質の“見える化”とツール適用の実際」
柿内博人氏（メルコ・パワー・システムズ株式会社　技術統括部）
大西康夫氏（日本コンピュウェア株式会社 営業技術本部 第二システム部）

第 6 回講演会（平成 20 年 1 月 17 日）
「企業におけるフォーマルメソッドの紹介」
劉　少英氏（法政大学情報科学部 コンピュータ科学科 情報科学研究科教授）

第 7 回講演会（平成 20 年 2 月 7 日）
講演 1「メモリリーク検出システム λ trace」
青島武伸氏（松下電器産業株式会社システムエンジニアリングセンター ソフト開発力強化第二チーム 主任技師）
講演 2「機能安全対応のためのソフトウェア安全分析手法」
長谷部浩二、水口大知（システム検証研究センター研究員）
平成 19 年度総会

および機器へのアクセス権限が与えられる一方で、十分なコンピテンシおよび独立性を備えていることが求められる。さらに評価にあたっては、故障解析等の手法・技法を、安全度水準に応じて選択しなければならないし、開発に用いられたツールも評価対象としなければならない。

以上のように、機能安全の評価・認証においては、広範な証拠と評価者の経験および能力に基づいた適正な判断が求められているといえる。これは IEC 61508 において示されているように、安全を達成するためには、様々な要因を考慮する必要があるためである。そして最終的には、全安全ライフサイクルを通じて作成された様々なドキュメントを証拠として、それらに基づく論理的な議論を組み立てながら、製品やシステムの安全性が主張されなければならない。特にソフトウェアについては、ハードウェアにおける偶発故障率のような客観的な数値データが示しにくいため、こうした安全性を主張するための議論の枠組みがより重要であると言えるだろう。そこでは実施された設計や検証作業が、どのような意図を持って行われたのか、そして、安全性に対していかに貢献するのかが問われることになる。こうした主張を伴う作業はいかにも欧米的で、日本人が得意とするところではないのかもしれないが、今後は積極的かつ柔軟な対応が必要であると考える。

システム検証研究センター　　水口 大知

■シリーズコラム「機能安全」全 3 回のご愛読ありがとうございました。今後取り上げてほしいテーマがございましたら、編集部まで お知らせ下さい。

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. 2

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。

■停まるかどうか

計算機の限界を表すのに、決定不可能という概念があります。決定不可能とは、『はい』『いいえ』を正しく答える固定したプログラムが存在しないこと、と言えばよいでしょうか。

例えば、「プログラムをみて、それがどんな入力に対しても正常に動作を終了するか」という問いは決定不可能です。プログラムの停止性と呼ばれるこの問題は、計算理論の教科書には必ず登場します。が、ときどき次のような証明を目にすることがあります：

[証明] プログラムの停止性を判定するプログラムMが存在すると仮定する。このプログラムMをサブルーチンに使って、次のようなプログラムＡを作る。

プログラムＡ：

任意のプログラムを入力とし、もし入力Ｐに停止性があるとMが判定するなら、Ａは無限ループする。Ｐに停止性がないなら、Ａは 1 を返して停止する。

仕様により、プログラムＡは自身を入力とすることもできる。しかし、Ａに停止性があるときＡは停止せず、Ａに停止性がないとき 1 を返して停止するので矛盾を生じる。したがってプログラムMは存在しない。[証明終了]

論理が簡潔なため、大学の初等科目の授業でもよく見かける論法です。しかし、「任意のプログラムを入力可能」という仮定の妥当性を議論しなくてよいのでしょうか。解説によっては、対角線論法を使うと断り書きがありながら、その証明に「プログラムの数が可算無限（自然数の個数と同数）」だという議論がでてこないこともあります。

■都合のいい議論

しかし、停止性の決定不可能性の証明の例は、へりくつを言うために出したのではありません。「知識や経験に差のある人に対して、もっともらしい議論を展開して目的の結論を得る。結論は正しいのだから嘘を言っているわけではない」という事例だと気づいて欲しいのです。数学的に正しい事柄は、誰がどんな解説をしようと結論は変わりません。結論の真偽を判定できない事柄なら、結論は無数にあります。だからこそ、人と話をした後などで、独りよがりな思考に陥っていなかったかどうか、振り返ってみるよう心がけたいものです。

■産総研 TODAY

話は変わりますが、イリノイにきてから「産総研ＴＯＤＡＹ」が手元に届くのを楽しみにしています。イリノイ大学日本人会の研究者 (計算機科学分野) のみなさんにも、産総研ＴＯＤＡＹは好評なようです。とくに、吉川弘之理事長の「高等大学院（AIST　SCHOOL）構想」の記事には、注目が集まりました。記事の内容もさることながら、産総研とは縁のない人たちが、吉川理事長の言葉（文章）に動かされるのを見て、話し方の手本がこんなにも身近にあったことに驚かされました。記事を読んでいる自分でさえ、吉川理事長の言葉を理解するのに必要な知識も経験も足りません。でも、そんな読み手に対してさえ、「研究所がこれからどういう一歩を踏み出すべきだと考えているのか」が伝わってくるのは、なんとも不思議なことです。「身近にある手本」は、少し距離をおいてみないと、見えてこないものなのですね。

■むすび

さて、イリノイでの在外研究も、残すところ三ヶ月余りとなりました。今回 (二回目) が滞在地から発信する最後の記事です。六月に帰国して、みなさんに会えるのを楽しみにしています。ご愛読ありがとうございました。

2008 年 2 月

システム検証研究センター　大崎 人士

Meseguer 教授（2 列目中央）を囲んで
Formal methods group のメンバーとともに

● ● ● ● ●

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 12 月～ 2008 年 2 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 定期開催しています。

日付	講演者（所属）
12/18	Jean-Pierre Jouannaud 氏（Laboratoire d'Infomatique, École Polytechnique）
1/31	西村　進氏（京都大学大学院理学研究科）
2/14	松野　裕氏（東北大学電気通信研究所）
2/21	高村博紀（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
（産総研コンソーシアム）

年間 6 ～ 7 回の講演会を開催しています。

第六回　2008 年 1 月 17 日（木）開催

講演者　劉　少英氏（法政大学情報科学部 コンピュータ科学科 情報科学研究科教授）

演　題　企業におけるフォーマルメソッドの紹介

概　要　ソフトウェアシステム開発の現状は、開発プロセスの厳密性が低く、開発されたシステムにバグが多く、修正に忙殺、コストが増大であり、厳しい状況である。この問題の主な原因としては、システムの要求がはっきり分からない、システム全体の構造および各部品の機能とそれらの間の関係を定義しないまま実装に入ってしまうことにある。この問題を解決するには、厳密性を保証するフォーマルメソッドが提案されている。フォーマルメソッドは系統的かつ厳密的な開発技術を示しているが、現実のシステム開発には実用性の疑問が問われている。本講演では、フォーマルメソッドを企業へ導入する問題点を説明した上で、企業で有効に応用可能なフォーマルメソッドを紹介する。特に、形式仕様記述技術の使い方、形式仕様に基づくソフトウェアの検査（inspection）およびテスト技術の使い方、モデル検査と形式的証明の役割、そしてフォーマルメソッドを導入するために必要な教育方法、導入後のソフトウェアプロジェクトの管理技術などを焦点に紹介する。

第七回　2008 年 2 月 7 日（木）開催

講演者1　青島武伸氏（松下電器産業株式会社　システムエンジニアリングセンター ソフト開発力強化第二チーム 主任技師）

演　題　メモリリーク検出システム λ trace

概　要　近年、家電製品に搭載されるソフトウェアはますます巨大化し、その品質を保ちながら、開発工数の増大の度合いを低く抑えることが大きな課題となっている。こうした背景のもと、我々はメモリリークの問題に着目し、ソースコードを対象に検査することでメモリリーク箇所を検出するシステムを開発した。本講演では、開発したシステムの設計・実装の内容を紹介するとともに、検査システムの実行環境、検査結果の精査環境などについてお話し、本システムの開発・運用を通じて考察した、現実のプロジェクトに寄与するための要件について述べたい。

講演者2　長谷部浩二、水口大知（CVS）

演　題　機能安全対応のためのソフトウェア安全分析手法

概　要　近年、多くのシステムがソフトウェアによって制御されるにつれて、ソフトウェアがシステムのリスク軽減のための安全機能を担うようになってきている。こうした安全関連システムのためのソフトウェア開発では、まず安全性に関する要求事項を抽出しなければならない。本講演では、そのための作業であるソフトウェア安全分析の方法について紹介をする。

【開催場所：システム検証研究センター千里サイト】

※平成１９年度は２月７日の第七回講演会を以って終了し、この日に総会を実施しました。現在平成 20 年度会員を募集中です。

詳しくはこちらから▼
コンソーシアムの URL：http://unit.aist.go.jp/cvs/conso-top.html

出版

◆テクニカルレポート

2008 年 1 月発行

PS-2008-001　システム検証研究センター
" モデル検査研修コース中級編 (Draft 版)"

PS-2008-002　システム検証研究センター
" 第四回システム検証の科学技術シンポジウム講演論文集 "

PS-2008-003　システム検証研究センター
" システム検証の事例報告集　2007 年度版 "

2 月発行

PS-2008-004
Satoshi Koike, Satoru Yoshida, and Hitoshi Ohsaki
"LTL モデル検査のための図示記法 "

PS-2008-005
Satoru Yoshida, Izumi Takeuti, Satoshi Koike, and Hitoshi Ohsaki
" 図示記法表現と LTL 論理式 "

※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

National Institute of Advanced Industrial Science and Technology AIST
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 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 Research Center for Verification and Semantics