National Institute of
Advanced Industrial Science
and Technology
AIST

AIST-PS-2009-002

ディペンダビリティ調査報告
2 月 22 日〜3 月 9 日
Newcastle, Edinburgh, York, Bath, London, UK

木下佳樹、武山誠、松野裕

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
(大阪府豊中市新千里西町 1-2-14)
独立行政法人 科学技術振興機構, CREST
(大阪府豊中市新千里西町 1-2-14)

算譜科学研究速報
Programming Science
Technical Report

Research Center
for Verification and Semantics

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 発行
Published by Research Center for Verification and Semantics
National Institute of Advanced Industrial Science and Technology

ディペンダビリティ調査旅行報告

２月２２日～３月９日

Newcastle, Edinburgh, York, Bath, London, UK

木下 佳樹、武山 誠、松野 裕

産業技術総合研究所システム検証研究センター

JST, CREST

1. はじめに

CREST プロジェクト「利用者指向ディペンダビリティ」に関して、ディペンダビリティに関する先行研究の調査のためイギリス国内の研究サイトを２００９年２月２２日から３月９日にかけて訪問した。訪問先は、Newcastle 大学の Cliff Jones 教授や Brian Randell 名誉教授のグループ、Edinburgh 大学の Don Sannella 教授のグループ、York 大学の Jim Woodcock 教授のグループ、Bath の Praxis 社、Bath 大学の John Power 博士、Swansea 大学の Monika Seisenberger 博士のグループ、 London の Adelard 社および City University of London の Robin Bloomfield 教授のグループの 8 箇所であった。

以下に日ごとに報告する。

２．ディペンダビリティ規格調査旅行

２月２３日（Newcastle 大学一日目）

Centre for Software Reliability, School of Computing Science, University of Newcastle (http://www.csr.ncl.ac.uk)に訪問した。

CLAREMONT TOWER

Newcastle 大学は Newcastle 中央駅から地下鉄で２駅、歩いても１５分程度のところにある。Jones 教授のグループがある Computing Science 学科は CLAREMONT TOWER と呼ばれる、近代的な建物の中にあった。


左から、木下、Cliff Jones、 武山

午前１０時に到着し、Jones 教授から歓迎を受けた。まず Jones 教授の教授室で以下のような内容の歓談をした。

- VDM の ISO 規格化 : ”unhappy experience” であった。皆、規格化は盛んなツール開発などにつながると期待したが、それほどにはならなかった。もちろんツール関係の努力はつづけられており、John Fitzgerald は日本の CSK と緊密に連携している。実はわれわれ CVS も現在 CSK と VDM に関係する共同プロジェクトを遂行しており、共通の知人もいた。
- Bosch との研究(後述の DEPLOY プロジェクトで行われている) : Requirements を突き止めるのに苦労する。requirement – specification – implementation のうち requirement と specification は性質に関わるべきものであるのに、企業の技術者は実装よりの下のレベルのことと混同しがち。 これは我々ＣＶＳでも同様の観察を得ている。Bosch に出向くときは、「それはドライバーの観点からはどういう性質なのか」といった質問で要求を聞きだしている。
- 扱いの難しい性質 :「スムース」＝「VMW のテストドライバーがスムースといったらスムース」。今は速度変化の性質として無理やり記述。
- 実時間系 : time granularityを考慮したAlan Burns(York)の “Time Bands”の考えは有益(see e.g. http://www.springerlink.com/index/p6483t20k808160u.pdf)
- Cliff Jones が主に執筆した Formal Methods の使用を定めた、現在唯一の規格であるイギリス防衛省の Defense Standard 00-55 Requirements for Safety Related Software in Defense Equipment は、現在 obsolete になっているという話であった。

その後継の規格である Defense Standard 00-56 Safety Management Requirements for Defense Systems は、現在改訂中であるが、Formal Methods は取り扱われていないようである。

歓談の後、場所を会議室に移し、研究グループの人々から研究内容の紹介を受けた。

１．　「Dependability Research at Newcastle,　Cliff Jones」

Cliff Jones 教授から Newcastle 大学で行われているディペンダビリティ研究の概要の紹介を受けた。School of Computing Science には、Dependability, Distributed Systems, Modelling and Reasoning, Scalable Information Management の４研究グループがある。Jones 教授率いる Dependability グループが dependability を非常に幅広く捉え、他の 3 グループと密接に連携している点が強調された。紹介されたプロジェクトのリストを以下に示す。

- 大プロジェクト
  - PDCS(Predictably Dependable Computing Systems), PDCS2
    - ESPRIT BRA(Basic Research Action)
    - http://research.cs.ncl.ac.uk/cabernet/www.laas.research.ec.org/pdcs/book/info.html
    - http://research.cs.ncl.ac.uk/cabernet/www.laas.research.ec.org/pdcs/index.html
  - DIRC(The Dependability Interdisciplinary Research Collaboration) (Dependability of Computer-based Systems)
    - EPSRC IRC. 5 大学、50 人超、6 年間、約８Mポンド。ニューキャッスル主導
    - http://www.csr.ncl.ac.uk/projects/projectDetails.php?targetId=102
    - 学際的アプローチに重点。(社会学:エジンバラ大､特に Donald McKanzie 教授、心理学：ニューキャッスル大、統計学：ランカスター大など)
    - 成果として 12 冊の本、500 本以上の論文が出版された。プロジェクトを通じて、産業界との強いつながりも生まれた。
    - 新世代の学際的研究者たちを育てたことも大きな成果。
  - DCSC (Dependable Computing Systems Centre)
    - BAE SYSTEMS 社、York 大と。17 年間継続。
    - http://www.csr.ncl.ac.uk/projects/projectDetails.php?targetId=18
    - 要求と仕様のモデル化と分析。特に timing problem, 要求の end-to-end traceability について。

- 従来プロセスがうまくまわらない理由のひとつは、各段階でのドキュメンテーション等の artifact について、作成の苦労をする人と使用して利益を得る人が一致しないこと。対策として、そのような artifact を各段階の成果物とする contractual obligation の強化を図った。これが BAE で成功し同社と良い関係が築けたことが長年にわたる協力を可能にした。

✧ DEPLOY (Industrial Deployment of Advanced System Engineering Methods for High Productivity and Dependability)
- http://www.csr.ncl.ac.uk/projects/projectDetails.php?targetId=260
- (後述 Romanovsky の発表に詳細)。

✧ ReSIST (Resilience for Survivability in IST)
- European Network of Excellence, 18 partners.
- http://www.resist-noe.org/
- 新規研究より成果普及が重点。
- ニューキャッスルは Dependability Explicit Computing(後述 Fitzgerald 発表に詳細)と Resilience Knowledge Database(後述 Randell 発表に詳細)。

✧ CSR Clubs (Safety-Critical Systems Club、Software Reliability & Metrics Club)
- 技術移転目的の NGO。Department of Trade and Industry による産学連携奨励を受けて 84 年から継続。800 社以上の有料"committed members", 2000 社以上のコンタクト。
- software reliability, measurement, safety concern を中心に。
- 活動内容:1 day seminar でのチュートリアル、トレーニング、啓蒙。short article を含むニュースレター発行、100－200 人を集める Annual Symposium など。

✧ TrAms(Trustworthy Ambient Systems)
- EPSRC "Platform Grant"。有力研究グループが競争的資金のプロジェクトの間を繋げることを可能にする、基盤的な使いよい資金。
  http://www.epsrc.ac.uk/ResearchFunding/Opportunities/Capacity/PlatformGrants/default.htm

➢ 小プロジェクト

✧ Hadrian(CyberCrime に対するもの。元 Detective Chief Inspector が CSR のメンバーとして参加している。)

✧ Captcha(Jeff Yang。オンライン登録時に歪んだ文字を認識させることで接続先が人間であることを自動的に判定するシステム。マイクロソフト、ヤフーの同様のシステムを破った研究で企業からも注目を集める。)

- ✧ Software System Engineering Initiative(SSEI)(Steve Riddle。DCSC の後継、BAE 社と。network 化、COTS、仕様・コンポーネントの変更、コンポーネント間の契約、アーキテクチャ記述・評価、acquisition monitoring 用メタデータ、等をキーワードとする点で DEOS と関係。英国防省資金。)
- ✧ VDM++研究（John Fitzgerald。仮想ネット上でハードリアルタイムの分散処理を離散時間・連続時間の hardware-in-the-loop, co-simulation で検証。高速複写機の事例。VICE ツール。Twente 大と。VDM に関する日本の CSK との協力は毎日曜日の会議など今も緊密。Fitzgerald は CSK の TradeOne, Felica 仕事でのモデル化にもに参加）
- ✧ FM-E グループ（John Fitzgerald。FM の主要国際会議開催。今年 11 月に Eidenhoven で“world congress”として FM2009 開催。）
- ✧ Atoms(Cliff Jones。“splitting atoms safely”。conncurrent system の開発において、atomicity refinement により従来の rely-guarantee 等以上の compositional development を可能にする。)

➢ UK Grand Challenge 6 “Dependable Systems Evolution”

- ✧ http://www.csr.ncl.ac.uk/gc6/, Cliff Jones on Steering Committee, John Fitzgerald, (Chair: Jim Woodcock(York))
- ✧ Hoare/Jones/Randell “Extending the Horizons of DSE (GC6)"へのRandellの参加がなければ、correctnessだけに関することで、dependabilityにもsystemにもevolutionにも関わらないものになるところであったとか。

➢ Dependability notion について

- ✧ Failure, Error, Fault の用語の選択は重要でないが、3 つの区別は重要
- ✧ 実際のシステムで state を把握するのは無理ではないかという質問に対しては、「どのシステムの話か明確にすることが肝要。さすれば、設計段階で考えるべき state はそこまで複雑にしないで済む。」との答え。

➢ DEPLOY Project について

- ✧ 次の Alexander Romanovsky 教授の発表で詳しく説明。

２．　「DEPLOY Project, Alexander Romanovsky」

Alexander Romanovsky

Alexander Romanovsky 教授から、EC Information Communication Technologies (ICT) FP7, call 1, Strategic Objective ICT-2007.1.2: Service and Software Architectures, Infrastructures and Engineering からの研究資金による、DEPLOY プロジェクト（http://www.deploy-project.eu/）に関する説明

を受けた。右がその様子の写真である。2008 年２月から 2012 年の１月まで行われる予定であり、17,885,406 ユーロの研究資金を受けて行われている。DEPLOY プロジェクトの目標は以下である。

・全体の目的は、形式的な工学手法を通じて、ディペンダブルなシステムのための、工学手法の確立に対し、主要な貢献をおこなうこと。

・ヨーロッパ産業の発展に真に貢献し、実スケールシステムの効率的な構築を助けること。

DEPLOY で開発される手法やツールを産業界で使われることをめざし、評価するための take-up を行うこと。

・システムのディペンダビリティと生産性の向上を明示すること。

Deploy プロジェクトは開始より１３ヶ月経過した段階にあり、産業技術者に対するブロック研修コースの開講、fault tolerance に関する研究などが行われているそうである。共同研究を行っている Bosch などの企業と、鉄道システムの検証について興味を持っているが、それにかかるコストが大変だ、などの議論を通して、実際の場を強く意識しながら研究を行っているそうである。われわれが参加している CREST プロジェクトが OS を主な対象としているところは異なるが、DEPLOY プロジェクトと目指す方向は似ていると感じた。同様な問題意識を持っているのだなと思った。

３．　「Dependability-Explicit Computing and Metadata, John Fitzgerald」


John Fitzgerald

システムが Service Oriented Architecture(SOA)により実装され、かつ複数の構成要素によりなるにつれ、システムのディペンダビリティを達成することは、open issue となっている。この研究では、そのようなシステムの開発、運用時に行う意思決定において必要となる情報を``dependability meta data”と名付け考察を行っている。Dependability meta data はセキュリティ、信頼性、性能などに関するさまざまなものを含む。例として、safety integrity level, failure rates, failure modes, pre- and post-conditions, MTBF, reliability, response time, resources consumed, component specification, fault assumptions, types of encryption、があげられている。Meta data をファーストクラスのデータとして扱いながらシステムの開発および運用を行うことを、Dependability Explicit Computing と名付け、それをどのようにすればいいのか、bio informatics のための e-Science システムとイギリスと中国にあるワークステーションによる BLAST システムについておこな

った。よく聞く話であるが、meta data、Dependability Explicit Computing などの言葉を作っているところがえらいと思った。

4．　「Models of Dynamic Coalitions, John Fitzgerald」

複数のエージェント（人間を含む）の動的な協調作業をどのようにモデル化するか、という話であった。相互作用の規則は動的に変化しうる。そのような相互作用を形式的にモデル化することを試みている。形式的なモデル化をベースとしてシミュレートするシステムを用いて、イギリスの Defense Science and Technology Laboratory で実験をした。

5．　「An approach to Deriving Specification, Manuel Mazzara」

Manuel Mazzara

Manuel Mazzara 博士から、ディペンダブルなシステムの、形式的な仕様を得るための完璧な手法を確立することを究極の目標とする、野心的な研究の説明を受けた。特にシステムの仕様が利用者の要求を満たすためにはどうすればいいか、という点に注目していた。そのための考察には、仕様を得るための 3 ステップ（UML,自然言語によるシステム境界の定義、時相論理などによる、システムに対する仮定の抽出、そして形式言語などによる仕様の導出）などがあった。最初のステップはシステムへの静的な観察により、次のステップは動的な観察による。システムの仕様を得る話を抽象的なレベルできれいにまとめており、今後参考になりそうな話であった。

6．　「Psychology of Programming, David Greathead」


David Greathead

心理学を専攻し、博士号をとったばかりの Greathead 博士による発表である。人間を心理テストにより１６種類に分類したところ、そのうちの１分類である「直感的」な人は、プログラムが得意であることがわかった。人を含むシステムディペンダビリティを考える場合は、心理学なども含む横断的な研究を行う必要があることはわかるが、実際に行っていることに、Jones 教授のグループの研究の広がりが感じられた。ただ、学際的な研究であるためか、なかなか適切な論文の投稿先が見つからないという悩みもあるそうである。

２月２４日（Newcastle 大学二日目）

午前１０時に到着。午前中は、木下によって産業技術総合研究所およびシステム検証研究センターの紹介、われわれのプロジェクト「利用者指向ディペンダビリティ」の方針説明を行われた。産総研の第 1 種基礎研究、第 2 種基礎研究、応用研究などの考え方に Jones 教授は興味をもったそうである。武山によって「Model-based testing of System LSI using Agda」の発表、および Agda の紹介が行われた。Mortin-Lof の型理論などに基づく Agda は、もはやメインストリームの研究ではないのでは、などの Jones 教授の意見などもあったが、武山の説明にある程度納得してくれたようである。

Brian Randell（左）

午後は Brian Randell 名誉教授による ReSIST プロジェクトに関する説明が行われた。Brian Randell 名誉教授は、ディペンダビリティ研究のパイオニアの一人として知られ、「Basic Concept and Taxonomy of Dependable and Secure Computing (IEEE Transaction on Dependable Secure Computing, 2004)」という、ディペンダビリティに関する基本的な文献として広く知られる論文の著者の一人である。Fault-Error-Failure の連鎖を最初に提案した。今回は、ReSIST（Resilience for Survivability in IST）と呼ばれるプロジェクトで開発された、セマンティックウエブシステムの紹介をしてもらった。ディペンダビリティに関する用語などは、人によって使い方が異なっていて、知識共有の点で問題があった。Randell 教授らが開発したシステムでは、関係する研究者、組織、プロジェクト、大学のコースなどの関係が図示される（http://www.rkbexplorer.com/）。データ数は、＜subject, predicate, object> の三つ組みが６０M 個あるそうである。われわれのチームの一員である和泉憲明はセマンティックウエブの専門家であり、このシステムについて彼に聞いてみたいと思った。

２月２５日（Edinburgh 大学）

Don Sannella（中央）

Don Sannella 教授のグループを訪問した。Edinburgh 大学の情報学部は、最近造られた新しい建物にある。新しい建物は、部屋がガラス張りであり、吹き抜けがあり、非常に開放的な雰囲気であった。午前中は Sannella 教授により研究内容の紹介が行われ

た。　Sannella 教授は、複数の研究資金を獲得しているそうである。主な研究内容は Proof Carrying Code に関するものであり、ユーザーの書いた Java ソースコードから、その正しさの証明つきの Java バイトコードを生成する。Java バイトコードはインターネット上を行き交うが、その Java バイトコードを使用する側は、安全なコードであるかを、それについてきた証明をチェックすることにより確かめる。Proof Carrying Code は１９９０年代後半に George Necula によって提案されたアイデアであるが、実用化にはいたらなかった。Sannella 教授のグループは、企業との共同研究を通じて実際に用いられることを目指している。Java VM のデモが行われた。Java VM を Coq で記述していること、Loop Invariant を最近提案された性能のよいヒューリスティックを用いて導出し、ユーザーが面倒な注記をコードに記述する必要をなくしていることなど興味深く、実用の可能性を感じた。午後は木下による産総研、プロジェクトの紹介が行われた。Sannella 教授は熱心に聴いてくれ、後で発表用のスライドが欲しいというリクエストをもらった。

Philip Wadler（左）

午後４時から武山らによる、miniTT という、Agda のできる限り小さなコア言語であることを目指した言語に関する発表が、情報学科のセミナーとして行われた。同じ時間帯に別なセミナーが行われていたにもかかわらず、部屋が満席になるほどの盛況であった。熱心に質問する人がいたが、Haskell、Java などで有名な Philip Wadler 教授であった。

２月２６日　（York 大学一日目）

York大学コンピュータサイエンス学部内

Cliff Jones 教授の紹介で、York 大学の Jim Woodcock 教授のグループを訪問した。今回訪問したグループすべてそうだが、多忙な中、多くの時間を割いてわれわれの訪問に対応してくれたことは大変感銘した。木下による産総研およびシステム検証研究センター、利用者指向ディペンダビリティプロジェクトの紹介のあと、Jim Woodcock 教授による研究紹介が行われた。

１．　「Grand Challenge in Verified Software,　Jim Woodcock」

Woodcock教授の専門はソフトウェア工学であり、特にFormal Methodsの適用に関する研究を行っている。Woodcock教授はまず、Tony Hoare, Bill Gatesなどの著名人がFormal Methodsの有用性を言っていることを紹介した。次にTony Hoareなどにより提唱されている「Verification Software Initiative」と呼ばれる、エラーのないソフトウェアを目指す、２１世紀のグランドチャレンジについて説明が行われた。その中には以下のようなパイロットプロジェクトが含まれる（http://asimod.in.tum.de/2008/Woodcock.pdfに詳細が説明されている）。

Jim Woodcock

・Mondex smart-card (Banach, Blackwell, Gogolla, Méry,Woodcock et al)

・POSIX-compliant flash file-store (Joshi/Holzmann,Woodcock/Freitas, Butler, Pronk, Kang, Ulbrich/Schmitt)

・Operating system kernels (Craig, Woodcock/Freitas)

・Pacemaker (Larson/McMaster, Oliveira2, Fitzgerald, SCC,ICSE 2009)

・FreeRTOS (Wittenstein, Ireland)

・Tokeneer (Praxis, Ireland)

・Radio spectrum auctions (Butler, He)

・Hypervisors (Microsoft, NRL)

FreeRTOS というのは、組み込みシステム向けの mini 実時間カーネルである。研究、商用に使えるそうである。Wittenstein という企業は、Eclipse ベースの FreeRTOS の Plug-in を開発した。RTOS を用いた研究が活発であることがうかがえた。

２．　「Justification for Floating-Point SPARK Analysis, Zoe Stephenson」

Zoe Stephenson

Zoe Stephenson 博士は、York 大学で Research Associate をしていて、ロールスロイスなどの企業との共同研究を主に行っている。われわれの訪問中常に同席していてくれた。Stephenson 博士は、浮動点少数演算に伴う、Bound Check 例外

の解析のための手法を開発した。この研究の面白いところは、その手法がいかに有用であるかを stake holder に説得するためのプロセスをも提案しているところである。Goal Structural Notation(GSN)という、樹形図のようにあることを主張するための strategy, assumption, justification などをその子供の木となるようなデータ構造を用いている。有用性を説得するというゴールを、その適切性、信頼性、妥当性の三つのサブゴールにわけ、それぞれが子供の木を構成している。解析手法のよさは、ベンチマーク性能や、false-positive 率の低さなどで示す論文が多いが、説得するプロセス自体も研究に含めている点でとても面白かった。

３．　「Verification of Control Systems using Circus, Ana Cavalcanti」

Senior Lecturer である Ana Cavalcanti 博士に、航空機や自動車で用いられる制御システムなどの検証を、従来個別に用いられていた仕様記述言語 Z やプロセス代数 CSP を組み合わせた記述法（Circus と名づけている）を用いて行っている研究を紹介してもらった。Circus を用いて、制御システム回路をリファインしていって、最終的に Ada という形式的な記述が容易なプログラミング言語に落として検証を行う。

２月２７日（York 大学二日目）

午前中は木下、武山によりシステム検証研究センターで行われている企業との共同研究、フィールドワークについての説明が行われた。訪問したいずれの大学でもそうであるが、企業との共同研究を重視している。センターで行われている共同研究に、とても興味を持っていただいた。

４．　「Model-Checking in the Early Lifecycle、Zoe Stephenson」

Zoe 博士による、システムライフサイクルの初期に、既存システムなど、そのとき得られる情報を基にモデル検査を行うことの有用性に関する研究発表。ライフサイクル全フェーズに対するディペンダビリティを考察しようとしているわれわれにとって、特にライフサイクル初期におけるモデル検査というテーマは、非常に興味深かった。

５．　「Evidence Based Certification, Tim Kelly」

Tim Kelly(中央)

最後に、Senior Lecturer である Tim Kelly 博士による、Safety Case の系統的な構築法および ISO/IEC 15026、Software Considerations in Airborne Systems and Equipment Certification などの System/Software Assurance に関する規格について発表があった。Kelly 博士は ISO/IEC 15026 規格策定に関するアドバイザリーボードの一員である。発表では、たとえば「Control System is Safe」のための Case（ここでは法律における、「証拠」の意味である）などを構築するために、GSN を用いていた。この方法は従来の「prescribe」な手法より利点があるそうである。また、evidence をどのように構築するのかなど、詳細に説明してもらった。あるシステムが Safe である、ディペンダブルである、などをどのように stake holder に説得していくのかが現在ディペンダビリティに関する研究において hot topic になっていることがわかった。今後のわれわれの研究の方向性に関して重要な示唆を得られた。

2 月 28 日に松野は帰国した。残りの一週間は木下と武山が調査を行った。

一週間滞在した Newcastle のホテルを後にして、Bath に向かった。Bath には Newcastle 大学の Cliff Jones 教授と DIRC プロジェクトを率いた Martyn Thomas 氏が設立した Praxis 社という、戦闘機などのミッションクリティカルなシステムの開発のカウンセリングを行う会社があり、Jones 教授の紹介で訪問した。

3 月 2 日 （Praxis, Bath）

Martyn Thomas

Bath 在住の独立コンサルタント Martyn Thomas 氏とともに Bath にある Praxis 社を訪問した。Praxis 社の事業を紹介されるとともに、CVS 紹介および DEOS 規格プロジェクトの概要を紹介、意見交換を行った。Praxis からは、Martyn Thomas、Keith Williams(Praxis High Integrity Systems Limited, Managing Director)、Andrew Vickers（Director, Praxis High Integrity Systems Limited, Head of Operations）、Rod Chapman（Praxis High Integrity Systems Limited, SPARK Products Manager）など、Praxis 社の幹部からワークショップ形式で説明を受けた。以下は時間経過を追ったものである。

13:00　Praxis 社に到着した。

13:15-14:00　　Praxis 社会議室にて昼食をとった。航空機事故への計算機システムの関わりについて、Peter Ladkin という人が詳しい、などの話を聞いた。日本の航空・鉄道事故調査委員会での取り扱いはどうなっているのか、後で調べようと思った。また、例えば Microsoft の SLAM から発展したソフトウェアは、できることは限られており、完全ではないけれども、C 言語などの主流の言語を対象に大量のプログラムを処理することができる。Praxis もその方向の技術的発展を考えるとよいのではないかなどの話も聞いた。さらに、情報システムの調達の、現行手法が根本的に間違っている。いきなり大規模の情報システム入札をするのではなく、まずアーキテクチャを対象に少額の入札を行い、その仕事をするアーキテクトがシステム利用者から事情を取材して形式的な仕様を書き、その仕様に基づいてシステム構築を再び入札する、という二段階のシステム調達に移行していくべきだ、という Praxis 側の説得にスコットランド行政府側は耳を傾け始めているそうである。あるいは DEPLOY プロジェクトでは SAP の参加に注目している、機能安全規格 IEC 61508 のソフトウェアパートはどうしようもない。ソフトウェア障害の確率、という概念がはいっているのがけしからん、などなど、興味深いことが得られた。

14:00-14:30　「Introduction to Praxis, Keith Williams」

Keith Williams より、Praxis の概要説明を受けた。Praxis は 1983 年に創業以来、安全系や高度目的システムなどのソフトウェア開発やリスク評価を行ってきた。その範囲は鉄道システムやエアバスなどの旅客機のエンジンなど、広範囲に及ぶそうである。

14:30-16:10 木下による産総研およびシステム検証研究センターの説明が行われた。

16:10-16:40 「Correctness by Construction and Lean Engineering, Andrew Vickers」

Andrew Vickers

Correctness by Construction(CbyC と略すそうである)とは、システムの構成の一歩ずつを、その正しさを確かめながら進める方式で、そのための具体的な手法が提供されている。Vickers はかれらの CbyC がトヨタの看板方式に似ていることを指摘した。

16:40-17:00 「SPARK Projects and Research Direction, Rod. Chapman」

Rod Chapman

SPARK Ada は Ada のサブセットで、Praxis は SPARK Ada 向けの静的解析ツール、とくに assertion の成立の静的解析を行う。コンパイラは特に用意せず、既存のコンパイラを用いる。静的解析ツールの研修コースを用意している。Adacore

http://www.adacore.com/home/ という、やはり安全系、高度目的システムの開発、コンサルティングを業務とする会社と提携しはじめ、Adacore のコンパイラや事業展開能力と協調できるようになった。

3 月 3 日、3 月 4 日は John Power 博士のいる Bath 大学において、Bath 大学、Swansea 大学とシステム検証研究センター共催のワークショップが開かれた。木下、武山による DEOS プロジェクトの概要の説明および企業との共同研究の発表が行われた。プログラムを以下に示す。

3 月 3 日 (Bath 大学)

11:15 Makoto Takeyama: Mini-TT

12:00 John Longley: Eriskay: a programming language based on game semantics

14:00 Yoshiki Kinoshita: Overview of DEOS dependability standard project

15:15 Anton Setzer: Coalgebras and Codata in Agda

16:15 Martin Churchill: A Concrete Representation of Observational Equivalence for PCF

3 月 4 日 (Bath 大学)

12:15 Yoshiki Kinoshita: Introduction to AIST, CVS and CFV

14:00 Makoto Takeyama: Model-based testing of System LSI using Agda

14:45 John Power: Towards a Geometric Foundation for Game Semantics

16:00 Yoshiki Kinoshita: Applications of Agda

http://wiki.bath.ac.uk/display/PMI2/Third+workshopにワークショップの詳細がある。

3 月 5 日、6 日（City University of London）

Newcastle 大学の Cliff Jones 教授の紹介で、City University of London の Robin Bloomfield 教授の研究グループを訪問した。ソフトウェアの信頼性評価、社会技術的側面からのシステムのディペンダビリティ、および Safety case など case(法律における、証拠などという意味)の構築方法などを主に研究している。Robin Bloomfield 教授は Cliff Jones 教授のグループとともに、DIRC プロジェクトに参加していた。1987 年に Adelard 社（http://www.adelard.com/web/index.html）を設立し、現在は、City University of London 内の Centre for Software Reliability (CSR)と同じ場所に Adelard 社のオフィスを置いている。Adelard 社もミッションクリティカルなシステムの開発のコンサルティングなどを行っている。所属はそれぞれ異なるものの、Adelard 社と CSR は表裏一体となってソフトウェアディペンダビリティに関する仕事を進めているように見える。参考に試用版をもらった、Adelard 社が創業のころより開発、販売している Assurance cases などを記述するツール ASCE を、以下に示すように大学の研究によく使っていた。

3 月 5 日の 10 時ごろ City University of London に到着した。まず木下から産総研およびシステム検証研究センターの紹介を行った。その後、Bloomfield 教授の研究グループから研究の紹介を 2 日に渡って受けた。紹介された研究を以下に示す。

1. 「[Un]dependable computer-aided decision making, Lorenzo Strigini」

Mammography(乳房 X 線撮影)を例にとって、人間がコンピュータの補助により操作を行うとき（Computer Aided Detection (CAD)）、間違いがどのように起こるのか（人間起因、コンピュータ起因、あるいは両方のせいでおこるのか)、またどのように防ぐのかに関する研究。CAD を使うとむしろ判断が難しくなる場合などがある。

2. 「Honeynet research briefing, Ilir Gashi」

1999 年より始まった Honeynet（http://www.honeynet.org/about）という、インターネットのセキュリティの向上をめざす非営利プロジェクトにおける Bloomfield 教授のグルー

プの研究の紹介。実際に動いているネットワークなどから、生のデータを取ってきてそれをもとにディペンダビリティの研究を行うという姿勢がよく現れていた。

3.　「 Preliminary Interdependency Analysis (PIA): An Overview,　Kizito Salako」

複数のシステムは複雑な相互依存の関係にあり、そのためひとつのシステムの障害が他のシステムに悪影響をもたらす。システムの相互依存の解析のために、ASCE などのツールを駆使して解析する手法、「Preliminary Interdependency Analysis(PIA)」を City University of London を中心として開発した。定量的、定性的解析を、システムのサービスのシナリオ、およびシステムの不確定要素のモデルを構築して行う。

4.　「Diverse redundancy for dependability (and performance) improvement, - A study with diverse SQL servers, - A prospective product/service in CSR Innovation programme,　Vladimir Stankovic」

Off-the-Shelf(OTS)（特に SQL サーバ）システムのディペンダビリティ（およびそれと相反しがちな性能)、に関する研究。SQL サーバーのディペンダビリテイを確保するためには、Fault Tolerance がよく用いられる。SQL の異なった実装を同時に用いる diversity の有効性を実証的な実験で測定し評価した。Diverse data replication によりディペンダビリティと高性能をともに得ようとする D-SQL アーキテクチャの設計を行っている。

5.　「Modelling Diverse Redundancy in Security,　Andrey A. Povyakalo」

4 の研究などに対する数学的なモデリングを行っている。

6.　「Multi-legged Arguments to Increase Confidence in Safety/Reliability Claims: A Bayesian Belief Net Study,　Bev Littlewood 」

システムがディペンダブルであるという主張の証拠など（dependability case）の正しさをどうやって確かめるか、ということに関する内容であった。Dependability Case とは仮定と証拠を元にした論理的推論であり、特定の confidence level での dependability claim を示すものである。ある主張のための仮定と証拠はその主張の子供の木となるような構造（Multi-legged）を構成する。それぞれの仮定、証拠がある確かさを持っているとき、それら全体の構造の確かさはどうなるかなどを Bayesian Belief Network を用いて数学的に考察していた。

7.　「Dependability Case for E-voting (Electronic voting),　Eugenio Alberdi」

Prêt à Voter という、電子投票システムのための dependability case の構築に関する研究。電子投票システムは高い信頼性が必要であり、また巨大であり、複雑な socio-technical なシステムである。電子投票システムのディペンダビリティ要求を Accuracy, Privacy, Successful Termination, Trustedness にわけ、GSN によって、dependability case を ASCE を使って書いていた。

8. 「Assurance cases, Robin Bloomfield」

City University of London で行われている Assurance case に関する研究の概要。Assurance case の役割は、risk communication とシステムを考える際のフレームワークを提供することにある。Assurance case に関する国際的な活動には International Working Group on Assurance Cases という closed な会合、ISO 15026 の規格策定、イギリス防衛省の Defense Standard 00-56 Safety Management Requirements for Defence Systems という規格策定などがある。研究は、原子力発電所などを対象に行っている。

9. 「Modeling dependency aspects of a hospital emergency department safety case using ASCE, Nick Chozos」

ASCE を使って、緊急医療部局のための safety case を、特に連続した障害の発生を考えてモデル化する研究の紹介。緊急医療部局のスタッフ、業務、医療機器、他の部局などの依存関係を ASCE で書いていた。上の３の研究のフィールドワークであるといえる。

10. 「Automated Proof with Caduceus: Recent Industrial Experience, Dan Sheridan」

原子力分野で使われるスマートセンサーの検証に証明支援系 Coq 上の Caduceus ツールを用いた事例研究。手法とツールの技術者から利点と欠点の報告が興味深かった。

３．まとめ

従事中の CREST プロジェクト「利用者指向ディペンダビリティ」に関して、ディペンダビリティに関する先行研究の調査のためイギリスを２００９年２月２２日から３月９日にかけて訪問した。Safety Case の構築法など、ディペンダビリティに関する、学際的、広範囲な研究内容に触れることができ大変有益であった。

いずれの研究機関でも強調されていたことは、

1. 企業と強く結びつきながら研究していること。Proof Carrying Code など、従来はアカ

デミックにとどまりがちであった研究テーマであっても、著名な企業との共同研究を通して、実際に企業に使ってもらうことを目標としていること、

2. Dependability を、心理学などさまざまな分野を横断する学際的分野として位置づけ、さまざまな分野の研究者の協力により行われていること、
3. Formal Methods を、dependability を達成するために必須のものとして扱っていること、

であった。

成果として、以下が得られた。

１．主に York 大学, City University of London などの研究グループで紹介された、システムが safe である、dependable であることの case（法律での意味で、証拠という意味で用いられる）をどのように構築するのかが、dependability の研究の中心的なテーマのひとつになっている。これは、われわれの「dependability をどのように評価するのか」に注目して研究を進めているアプローチに近い。

２．各研究グループとのコネクションが得られた。特に Cliff Jones 教授、Jim Woodcock 教授のグループは産総研およびシステム検証研究センターの研究に興味を持ってくれ、今後共同研究を含めコンタクトを続けることになった。また City University of London の Robin Bloomfield 教授が主催している、アメリカのワシントンで、closed で開かれている International Working Group on Assurance Cases にシステム検証研究センターから研究員を参加させることになった。ディペンダビリティに関する規格をつくるための一歩になった。

ディペンダビリティ調査報告　2月22日〜3月9日　Newcastle, Edinburgh, York, Bath, London, UK
(算譜科学研究速報)
発行日：2009年5月22日
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)
同連絡先：〒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
TEL：06-4863-5025
e-mail：informatics-inquiry@m.aist.go.jp

Dependability Survey Trip Report　2009/2/22 – 2009/3/9　Newcastle, Edinburgh, York, Bath, London, UK (in Japanese)
(Programming Science Technical Report)
22 May 2009
(Research Center for Verification and Semantics (CVS))
National Institute of Advanced Industrial Science and Technology (AIST)
5F Mitsui Sumitomo Kaijo Senri Bldg., 1-2-14, Shinsenrinishi-machi, Toyonaka, Osaka 560-0083 Japan
TEL：+81-6-4863-5025
e-mail：informatics-inquiry@m.aist.go.jp

AIST01-J00022-92