特集
フォーマルメソッドの新潮流 2

Part II：産業界への応用

フォーマルメソッドのフィールドワーク

木下佳樹　高井利憲　大崎人士
●（独）産業技術総合研究所システム検証研究センター

フィールドワークとは

フィールドワークという語は元々民族学などでの専門用語で，野外研究と翻訳される．村落などの社会を観察し，それを説明する枠組みをつくる研究，といってよいだろう．産業技術総合研究所システム検証研究センター（AIST/CVS）では，この言葉にかなりの拡大解釈をくわえて，科学者が自らの専門知識と技能を用いて一般社会ではたらく意味にもちい，フィールドワークと科学研究の二本立てで，研究活動を進めている．フィールドワークをとおして社会に貢献するだけでなく，その経験から科学研究の新しい豊かな対象をうみだすことができるかもしれないとの期待をもって活動している．なお，産業技術総合研究所は，第一種の基礎研究，第二種の基礎研究，製品化研究などからなる本格研究を推進しているが，第一種の基礎研究がほぼ科学研究に対応し，フィールドワークは第二種の基礎研究の１つの方法として位置づけられる．

●参加者に資するもの

我々研究者側がフィールドワークにもとめるものは，具体的な事例の獲得である．検証技法にかぎらず，ソフトウェア開発技法を大規模な開発に適用するためには，研究室内の実験では十分でなく，どうしても，開発現場での事例にふれた体験と，事例の分析が必要である．フィールドワークはまた，我々の科学研究におけるテーマ選択にもよい影響をあたえるだろうと期待される．学術の世界にとじこもるだけではなく，社会と相互作用しつつすすむ科学研究を目指す我々にとって，フィールドワークは，外界との接点として重要である．

他方，共同研究のパートナーが，フィールドワークから得るものは，自らの仕事に適応させた形での先端技術の移転である．数理的技法を開発現場に導入するには，教科書にかかれた知識だけではたりない．基礎的な知識を，その場その場に適応した形に定型化する必要がある．また，現場の技術者が新しい技法をまなび，新たに発生する作業を身につける必要があるかもしれない．研究所は，フィールドワークをとおして，最新の技術をその適用現場に沿った形にして提供することができる．

●具体的な課題提示

数理的技法に関係しそうな具体的な課題をフィールドがAIST/CVSに提示するところから，フィールドワークがはじまる．数理的技法がその課題に有効なのかどうか，前もってフィールドの側で分かるわけではない．それが判断できるくらいなら，はじめから研究所の助けを借りずに技術導入していたはずである．この段階では，検証に直接関係しない開発現場の専門用語や概念を数理的技法の研究者側が理解する必要がある．これは一般には容易ではない．フィールド自身が研究所を持っていれば，開発部門とAIST/CVSの間の通訳としてはたらくことができて好都合だろうと思われる．

課題が具体的かつ詳細にAIST/CVSの研究者の前に提示されたら，モデル検証法，対話型検証法など，多数ある数理的技法のうちのどれをもちいるべきかを研究者が検討してきめ，それをフィールドの現場に適用する．現場への適用が肝心だから，現場が新しいテクニックを利用することに対して肯定的にならないと，この段階がすすまない．

●縁側から奥座敷へ

大抵は，AIST/CVSが縁側に入れてもらうことからはじまる．つまり，初めての適用では，すでに開発が終了しているソフトウェアや，昔作ったプロトタイプなどに対する検証を行ってみせることからはじまることが多いのである．記録にのこっている不具合が，数理的技法でみつかるかどうかをみたりもする．

これをくりかえすうちに，AIST/CVSの研究者および数理的技法へのフィールドの人々からの信頼が増し，次第に縁側から奥座敷へととおしてもらえるようになる．

奥座敷とはすなわち，フィールドにおける本格的開発計画，企業であれば，待ったなしの納期が設定されているような開発案件である．そこでフィールドワークを行えるようになって初めて，技法を現実の大規模開発に適用するときの問題点が明らかになり，必要な研究を追加したり，技術者の教育方針を修正したりといったアクションをとることができる．

●成果の発表

フィールドワークから得た知見は，知的財産ではなく学術的な知識だから，学術誌などに発表して研究コミュニティで共有すべきである．しかし，フィールドワークによる野外科学の研究のすすめ方は，実験科学や書斎科学とは異なるので，発表の手順や問題点に自ずから異なるところがいくつかある．

まず，共同研究先の開発過程あるいはそこで稼働しているシステムを題材に使う研究なので，題材自体に共同研究先の重要な秘密情報が含まれている場合が多い，という問題がある．発表前に共同研究先との十分な打ち合わせが必要である．また，この打ち合わせをスムーズにすすめるには，共同研究開始時に必要な条項を契約書に記しておくことが有効である．たとえば，開示情報についての合意を発表のたびに行うのかどうか，また，秘密情報に関しても，永久に秘密とするのか，一定の年月の後には開示してよいのかどうか，開示してよいとしても合意の上で開示するのか合意が必要ないのか，などという点である．

題材に秘密情報が含まれるといっても，それは大抵の場合，遂行中のフィールドワークとは直接関係ない情報である場合がほとんどである．たとえば，DVD プレーヤの組込みシステムを検証するフィールドワークにおいて，再生画像の美しさに関するノウハウは，プレーヤを開発するメーカにとっては重大な秘密情報になり得るが，プレーヤの動作検証を行う立場からは，あまり興味のない情報である．検証に直接関係のない企業秘密をうまく隠蔽しながら検証の様子だけを発表することは，容易な場合が多い．一方，不具合そのものは，大抵の共同研究パートナーにとって，重大な秘密情報である．製品情報をうまく隠蔽しながら，不具合の本質を浮き彫りにするようなプレゼンテーションには工夫が必要である．不具合の実例の本質的な部分を産業界および学界で共有することができるとすれば，社会全体のシステムの信頼性向上にとって大きな利益となる．

●臨床研究としてのフィールドワーク

フィールドワークは医学でいう臨床研究と同様で，短期間で成果を得ることがむずかしく，フィールドワークの観点からは重要な論点も，既成ジャーナルの価値基準に当てはめると重視されないものとなりがちであるため，論文の出版がむずかしい．学位を早急に取得しなければならない学徒には困難な道といえよう．しかし，産学連携を真剣に求めるとすれば，フィールドワークあるいはこれと似たような活動が，産業界を含めた社会における問題の解決に最も効果的なのではないだろうか．

フィールドワークの事例紹介

本章では，AIST/CVS の設立以来，これまでに携わった事例のうちから，典型的なものを 3 件えらんで紹介する．自動車，精密機器，製造機器などの組込みシステムに関するものばかりである．ソフトウェアの信頼性向上への要求が，組込みシステムの業界において特に強いように感じられるのは興味深い．この理由を本格的に調査してはいないが，元来機械やハードウェアに対しては信頼性への要求がソフトウェアに対してよりも強いため，ハードウェアとソフトウェアの境界を扱う組込みシステムの世界でも，自然に高い信頼性を求めるものとみている．今後は伝統的なソフトウェアの世界で，より高い信頼性を求めるのが一般的になるかもしれない．

(1) では，矢崎総業グループにおけるシステム開発過程の信頼性をさらに向上させるため，モデル検査手法の導入実験を行った経過を紹介する．これは 6 年間にわたる共同研究の中間成果というべきものであり，個別の検証事例がこの研究から多数生まれているが，それらはすでにさまざまな機会に発表済みである．本稿では，この共同研究でこれまでに得られた成果を概観して考察をくわえる．

(2) は特定の不具合の解析にモデル検査を用いた事例である．ハードウェアおよび機械部分を含めたシステム全体の挙動の中に不具合が観察された，という例に関して，アセンブリ言語で書かれたソースコードと仕様書，ハードウェアの仕様書，不具合の観察記録などの提供を企業から受けて，不具合の挙動の原因をモデル検査によって調べたものである．

(3) は開発が終わってから検証するのではなく，開発過程に検証過程を埋め込み，相互に入り組ませた開発・検証過程の実現を試みた事例である．不具合をいくつか検出したが，検証を行う我々は，検証にとどまらず，開発にも参加した．検証と開発は，交互に行われながらすすんでいくもので，両者をきれいに切り分けることができない，という我々の直観を裏付ける事例ともいえる．

(1) 数理的技法の導入による信頼性向上を目指して

はじめに紹介する事例は，車載組込みソフトウェアの

品質および信頼性向上に関する矢崎総業グループ（以下では矢崎総業）との共同研究である．我々にとってのこの共同研究の目標は，モデル検査技術の製品開発の現場におけるフィージビリティを確かめることである．一方，反例の出力によるバグ発見を特徴とし，ツールも整備されつつあったモデル検査は，数理的技法の中でも最も実用化に近い技術であるとの予想が，共同研究開始当初から産業側にあった．

共同研究当初は手探りの状態で，文献などの調査からはじめたが，すぐに実地に試してみようということになり，まず過去に開発されたプロトタイプを対象としてモデル検査による検証を行ってみた．その過程でしだいに産業側からの信頼を得，次は，過去に開発された製品(プロトタイプではない)を対象として同様のことを行った．不具合の記録が残っているので，それを我々には隠してもらい，その不具合がモデル検査によってみつかるかどうか，といった一種のブラインドテストを行ったりもした．結果が良好だったので，さらに，新製品の検証を，従来手法による検証と並行させて行う，といった試みも行えるようになった．「縁側」から「奥座敷」にしだいに移っていったのである．

開発現場のさまざまな開発工程で，モデル検査による検証を行う適用実験を繰り返した．共同研究の途中からは，開発過程のいわゆるＶ字モデルにもとづいて考えるようになり，要求分析，基本設計，詳細設計，実装の各工程で適用実験を実施した．検査対象も，開発が終了したものから，既知のバグの存在するものや存在しないもの，開発途中のものなど，さまざまであった．それらの実験の過程から，モデル検査を開発現場に導入するための観察をいくつか得た．その中から３つを紹介する．これらの観察はこの事例に対するものであるから，どこが一般的なもので，どこがこの事例に特別なものであるか，ということの分析は今後をまたねばならない．

観察の１つ目は「モデル検査の効果は，下流工程の実装段階の検証におけるほうが高い」ということである．一般には，モデル検査をはじめとする数理的技法は上流工程に使うのが有効だとされる[13]．我々も，他のプロジェクトにおいてはそのような観察を得ている．仕様の設計などの上流工程における間違いの方が，手戻りが生じた場合のコストが大きいことや，実装などの下流工程ではそのままモデル化すると，状態爆発をひきおこしやすいなどの理由からであろうと思われる．しかし，ソフトウェアの品質向上をはかるためには，上流工程に導入したモデル検査技術に合わせて，他のソフトウェア開発工程も変更する必要がある．このような変更のコストを合わせてかんがえると，モデル検査導入の効果の判定は複雑でむずかしい．不具合がみつかるという局所的な便益だけをみて，上流工程へのモデル検査が有効だという結論を安易に出すことはできない．

本事例では上流工程での仕様書の検証と下流工程での実装の検証の双方にモデル検査を適用してみた．その結果，上流工程への適用では，現実を十分反映しないモデル構築，という問題点が大きく，下流工程への適用では，状態数爆発の問題点が顕著であることを観察した．

現実を十分反映しないモデルを構築してしまうのは，暗黙知として個別の技術領域の中で共有されている領域知識をソフトウェア技術者が持っていないことが，大きな原因である．領域知識の暗黙知化の問題は深刻で，パートナー企業所属のソフトウェアエンジニアですら，しばしば個別の担当者に仕様書の詳細についての疑問を問い合わせる必要があった．一方，状態爆発に関しては後に述べる環境ドライバ法により，部分的な解決をみた．その結果，モデル検査の適用がより高い効果を上げたとの判定が，パートナー企業との議論によって得られた．

上流工程へのモデル検査の適用実験においては，モデル化にかかる時間の短縮が課題であった．上記のように，業界特有の領域知識が必要であるため，上流工程ではモデルの作成が困難であった．仕様書から，モデル検査ができる程度のモデルを作成するためには，開発者への聞き取り調査を実施し，検査対象に関する情報を十分に得る必要がある．しかし，研究所にいるモデル検査の担当者と，企業内で開発を担当するエンジニアとが意思疎通をするのは，用語や背景知識や概念の共有が十分でないために，困難であり，かつきわめて時間がかかる．また，開発担当者は開発作業に多忙だから，共同研究参加者からのインタビューに長い時間をかけて応じることができるとは限らない．

モデル検査によって，仕様書の中の記述漏れや不整合を指摘しても，領域知識の不足によりモデルを構築する際に現実を十分反映させていないことが原因であることも多かった．領域知識に関する暗黙知を共有しない第三者が，上流工程で作成された資料に対してモデル検査を行い，どのような情報がさらに必要となるか，という実験も行った．

一方，下流工程の実装段階では，ソフトウェアの仕様はすでにプログラミング言語などの形で形式化されており，背景知識が不足していても正確な理解が可能である．また，システムのハードウェアや外界の知識が得られていれば，振舞いを再現することもできる．さらに，開発現場も，実装段階での品質向上を望んでいた．そこで，ソースコードレベルでの実装段階の検証を試みることにした．ソースコードのモデル検査では，状態数の爆発が課題であることはよく知られているとおりである．

そこで，状態爆発問題を解決する方法を模索し，何

回かの適用実験を通して，環境ドライバの概念を導入し，これにもとづく検証シナリオを開発した[4]．環境ドライバ法は，周期駆動型システムのモデル化を，状態爆発を起こさないようにつとめながら行う手法である．この手法によって，検査期間と検査に必要な人員を見積もることができるようになった．さらに，モデル検査をいくつかの工程に分割し，分業体制でモデル検査工程を実施できるようになったことも大きな利点である．また，周期駆動型システムは，制御システムにおける代表的なソフトウェアアーキテクチャの1つであるから，環境ドライバ法は，組込みシステムをはじめとする制御システムに広く応用することができる．なお，環境ドライバの概念は，フィードバック系における「外界」，HILS（hardware in the loop simulation）における「ループ」にほぼ相当するが，尾崎らはそれらとは独立にこの概念を導入した．また，環境ドライバ法における状態数削減の手法は，いわゆる cone of influence reduction と関連すると思われる．

「最も時間を要するのは，検査対象の理解および検査項目の決定である」というのが，この事例から得た2番目の観察である．すでに述べたように，検査対象の理解が困難であることは定性的に理解されていたが，工数分析の結果，この工程に実際に工数がかかっているという結論がでた．一般に，モデル検査による検証シナリオは，1)検査対象の理解および検査項目の決定，2)検査対象のモデル化および検査項目の翻訳，3)モデル検査，4)反例解析の4つの段階から構成される．この中で，2)，3)は，共同研究の進展によるノウハウの蓄積や技術者への教育を通じて，時間を短縮することができた．また，4）は適当なツールの導入で大幅な時間短縮が可能だと思われる[12), 13)]．しかし，特に，検証技術の研究者など，開発のフィールドの外の者が検証を担当する場合，検査対象の理解に最も時間を要した．開発者と知識の共有が十分でないことが主な理由であろうとかんがえられる．さらに，検査対象を十分に理解した上でも，検査項目を取捨選択する過程は，その後の検証工程の見通しや検証工数の見積もりにも関係するため，多くの時間をかけて行った．検査項目を取捨選択する工数を減らすための工夫も，いくつか得られた．

領域知識の伝達の手間をかんがえると，開発過程の一部としてモデル検査による検証を行う場合には，検査対象を開発している技術者自身，またはそれに近い者が直接モデル検査を行うのが適切ではないかとかんがえられる．そのためには，ソフトウェア開発技術者に対してモデル検査などの検証技術の教育を施すことが必要である．本共同研究の中だけでも数多くのモデル検査の教育プログラムを実施し，また後述するように，AIST/CVS では，一般技術者向けの研修コースも開発している．

3つ目の観察は「多くのソフトウェア技術者にとって難しいのは遷移系の記述ではなく，検査項目の記述である」ということである．遷移系の記述は行数が多いが，必要な概念はプログラミングにあるので，ソフトウェア技術者にとってほとんど困難はない．しかし，検査項目の記述は，時相論理の論理式でなされなければならず，大抵のソフトウェア技術者は習得に苦労する．時相論理の論理式の意味は無限列や無限木の集合で与えられるが，無限の概念に関する数学的リテラシーの不足が，ここでの苦労の原因の本質であるとかんがえられる．このような課題を克服するソフトウェア技術者教育が求められる．

時相論理に対する現場技術者の心理的ハードルだけでも低くしようと，我々は検査項目に対する直観的な理解を促す図的な表現，すなわち図示記法を考案した[2)]．特に時相論理 LTL の部分クラスに対する図的な表記法を定式化した[3)]．図示記法を用いることによって，検査式の作成の習得やデバッグの心理的難易度を下げ，検査内容を伝達するためのコミュニケーション手段を得ることができた．真に必要な数学的リテラシーがソフトウェア技術者の間に広がるまでの間の過渡的な知的道具として，あるいは初学者のための簡易な導入法として，図示記法は有効であるとかんがえている．

以上に記したような共同研究を，2002 年以来 6 年間にわたって遂行し，数理的技法を現場導入する際の必要条件である検査工数の削減に成功した．13 回にわたる適用実験を行った結果，初期の事例では，2 カ月程度の時間を要した検査実験が，2005 年度には，9 日間で終了することとなった[4), 5)]．

(2)不具合解析を目指して

2つ目の事例は，ソフトウェア，ハードウェア，機械部分のすべてを含めた組込みシステムの不具合解析に，数理的技法を適用する試みである．ハードウェアの故障解析手法にはいくつかの定石があり，対象を限定すれば解析のシナリオが確立されている場合も多い．しかし，ソフトウェアの不具合解析のシナリオは，未だ定まっているとは言いがたい．通常のデバッグ技術や，テスト，レビューなど，要素となる手法はあるが，それらをどう組み合わせるのか，また，これらの手法だけで十分なのかどうかなど，未開拓の部分が多い．

ある企業(以下パートナー企業)が，ある組込みシステムの原因不明の不具合の解析を，AIST/CVS に相談したことが共同研究開始のきっかけとなった．不具合の現象は実機テストにより確認できるが，原因がどこにあるのか分からず，機械部分にあるのか，ハードウェアにあるのか，ソフトウェアにあるのかすら不明であった．不具合が観察された組込みシステムは，ハードウェアに関し

ては徹底的に調査を行い，ソフトウェアに対しても，テストやレビューにより，不具合解析を行っていたが，原因究明にはいたっていなかった．AIST/CVS としても，テストやレビューではできなかったことが，数理的技法により初めて可能になるとすれば，数理的技法の有効性を示すよい材料になるとかんがえ，共同研究を開始した．3 カ月の共同研究遂行の結果，不具合の全容解明にはいたらなかったが，ソースコードにおいて，アドレッシングモードの間違いをモデル化の過程で発見した．この経験から，数理的技法を効果的にもちいることにより，ソフトウェアの不具合解析に限らず，安全性をはじめとするいろいろな性質を分析するためのシナリオを開発することができるのではないかとかんがえている．

この事例で不具合解析の対象としたのは，ソフトウェアである．ソースコードは約 1 万行のアセンブラで記述されたプログラムであった．また，ソースコードとほぼ対応するような詳細なフローチャートが存在し，解析過程で参照することができた．ほかに，ハードウェアの仕様書，および不具合の観察記録も参照した．ソースコードを，人手によって適宜抽象化しながらモデル検査器 Spin によってモデル検査した．フローチャートではなく，状態数爆発をひきおこしがちなソースコードを，あえてモデル検査の対象としたのは，テストやソースコードや仕様書に対するレビューでは不具合が検出できず，ソースコード上の微妙な間違いが不具合をひきおこしていると予想したためである．

解析はアセンブラプログラムを対象とする段階と，フローチャートを対象とする段階の 2 段階にわけて実施した．まず，アセンブラのソースコードすべてをモデル化し，モデル検査をするという方針ではじめた．アセンブラプログラムを半自動的に Promela に変換することも行った．アセンブラのコードを Promela に変換する簡単なプログラムを Perl で実装し，変換されたものを必要に応じて修正する半自動的な変換によりモデルを作成したが，このような素朴な方法で作成したモデルでは簡単に状態数爆発を発生させてしまい，Spin の通常モードではなく，シミュレーションモードでしかモデル検査ができなかった．したがって，ソースコードを忠実にモデル検査したわけではない．

しかし，このモデル化の過程で，値とアドレスを取り違えるアドレッシングモードの間違いを発見した [6]．これは，ソースコードをモデル記述言語で記述しようとしたことから発見されたものだから，モデル検査によって発見したというよりも，形式記述という行為の直接の効果によって発見したといえるだろう．なお，Spin のシミュレーションモードをもちいて，上記の間違いのあるコードに実行が到達する可能性があることも，実行パスを提示して証明できた．したがって，このコーディングの間違いはバグと呼ぶに値するものであるといえる．

第 2 段階では，ソースコードではなく，フローチャートから我々が抽出した抽象的な遷移系を対象に解析をすすめた．発見されたアドレッシングモードの間違いによるバグが，報告された不具合につながるか否かをしらべるのが目的である．バグに関係する部分をフローチャートから抜き出した抽象的なモデルを対象に，報告された不具合が発生するか否かをモデル検査によってしらべた．反例が得られれば，対応する実機上での実行パスをしらべ，ソースコードの上での不具合解析を続けることができる，というシナリオである．しかし，反例が得られなければ，その後解析のすすめようがなく，アドレッシングモードの間違いが不具合の原因であるとも原因でないともいえない，ということになる．

検証作業の結果，反例は得られなかった．したがって，アドレッシングモードの間違いと不具合との因果関係は不明なままである．けれども，フローチャートから抽出した抽象的な遷移系のレベルでは，両者の因果関係がない，ということを以下のようにして考察することができる．実機で稼働しているアセンブラのソースコードプログラムとフローチャートプログラムとの間に模倣関係があるかどうかまでを証明することができていないので，この考察からすぐにアドレッシングモードの間違いと報告された不具合との間に因果関係がないと結論することはできないが，因果関係がないことの蓋然性を与える材料にはなる．

さて，フローチャートから抽出した抽象的な遷移系のレベルでアドレッシングモードの間違いと不具合の因果関係の有無を調べるために，まず，もとのフローチャート F にアドレッシングモードの間違いを埋め込んだ．このフローチャートを F' とする（図 -1）．いわゆるスライシングのテクニックを用いて F' から抽象モデル A' を抽出し，状態数削減を試みた．この抽象モデル A' が報告された不具合をもたないことをモデル検査によって検査したところ反例は得られず，A' は不具合をひきおこさないと結論した．一方，A' と F' がどのような関係にあるかをしらべ，両者が足踏み同値（stuttering equivalence）[8] の関係（いわゆる弱双模倣 weak bisimulation と同義）にあることを確かめた．足踏み同値なモデル間では，next 演算子を含まない LTL を保存していることが知られている．F' が反例を持たないので，今回発見したバグと報告された不具合の間には因果関係がないと結論した [7]．

さて，さらに，パートナー企業側が挙げていた別のソースコード上の原因候補をモデル化し，それらが報告不具合にどのように影響するのかの解析もモデル検査を用

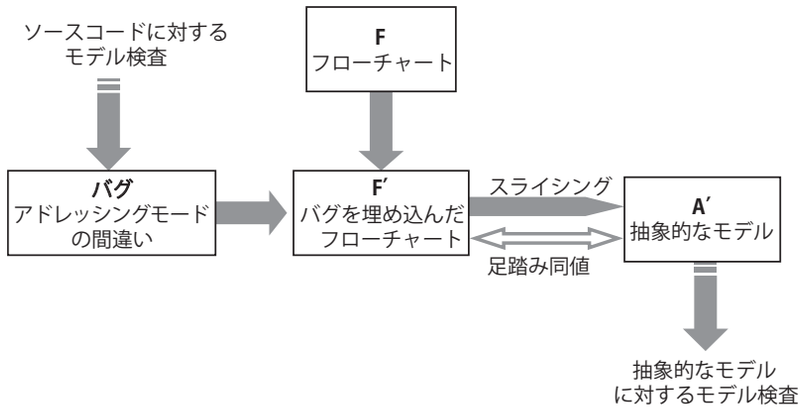

図 -1　不具合解析事例におけるフローチャートの解析

いて行った．その結果，不具合間の因果関係を明らかにすることができた．

上記の考察は，抽象的なモデルを注意深く作成して検査することにより，抽象的なレベルにおいてソフトウェアモジュールを不具合の原因候補からはずすことに，一定の根拠が得られることを意味する．ここで鍵になるのは，模倣関係の概念である．本研究のシナリオを普遍化して，一般的な不具合解析シナリオを作るのは今後の研究課題である．

本プロジェクトは，企業との共同研究として行ったが，期間が 3 カ月と短く，リソースも十分には得られなかったこともあって，不具合の全体像を明らかにすることはできなかった．遷移系モデルに不具合を埋め込んでモデル検査し，不具合の原因解析を進めるというシナリオには臨床医学とのアナロジーがあり，示唆的である．

(3) 開発と検証の融合

最後の事例は (株) イシダとの共同研究である．産総研からはシステム検証研究センターだけではなく，グリッド研究センターからも参加者を得た．フィールドワークの枠組みで，検証だけでなく，実際のソフトウェアの開発も行い，その傍らで検証も行ったというものである．検証に関しても，モデル検査のみならず，形式的な定理証明による検証も導入した．工場機器に対するセキュアな自動遠隔ソフトウェア更新システムのプロトタイプの開発過程の中にさまざまな数理的技法による検証を埋め込み，システムセキュリティの信頼性を総合的に上げようとする野心的なプロジェクトであった．

対象システムは，工場機器の自動遠隔ソフトウェア更新システム，すなわち工場内の組込み機器のプログラムの更新を，インターネットやイントラネットを通じて提供するものである．システムの満たすべき性質の中で，今回検査対象としたものは，更新プログラムが改竄されないこと，更新プログラムが最新であること，などのセキュリティに関する性質である．設計および開発は，暗号系などを提供する既存のコンポーネントを，セキュリティ上の性質を考慮しつつ組み合わせて行った．これらの既存のコンポーネントの秘匿性や認証性を仮定すればプログラムに関する上記の性質が成り立つことを検証した．

開発はまず，プロトコルの設計から始めた．実際の製品で使用するプロトコルに対して，検証技術によるだけでなく，不具合のない利用実績を考慮した proven by use の観点からもセキュリティに関するアドバイスをしながらの開発となった．数理的技法による検証は，以下に紹介するプロトコル仕様に対する検証のほかに，ソースコードに対するモデル検査 [11] を行っている．

まず，形式的な (しかし人手による) 定理証明にもとづく検証を，BAN Logic をもちいて行った [9]．一定の枠組みのもとで，改竄の検出可能性を証明した．また，更新ソフトウェアが最新でない場合があることを，反例を与えてしめすことができた．そして，更新ソフトウェアを常に最新のものに保つための実施可能な改善案を BAN logic における有効性の証明とともにしめした．

次に，上記定理証明による検証を行った考察をもとに，モデル検査によってプロトコルの認証性，つまり通信手順のせいで，偽のデータを受け取ってしまうことがないか，相手に成りすました他人と通信していることがないか，などといったことを検証した．モデル作成の段階で，不正な工場機器が存在する場合には，誤った更新プログラムを受理する可能性が明らかになった [10]．モデル検査によって新たな問題は出現しなかったが，上記問題や，仕様書のレビューの段階で発見した問題を，モデル検査器の上で再現することが，共同研究参加者間で情報を曖昧さなく正しく共有する上で有益であった．これらの発見されたバグの情報にもとづき，プロトタイプの改良につなげた．

このプロジェクトでは，モデル検査および定理証明な

ど複数の検証手法の適用をこころみ，検証の結果をプロトタイプ開発に反映させることができた．その結果，定理証明による検証で得られた結果をどのように開発現場で位置づけるかという問題が課題として残された．つまり，モデル検査に比べて，定理証明の開発現場への導入は，より困難であると思われる．モデル検査では，命題が成り立つという情報か反例が得られるが，どちらも論理学になじみのない者にもよく分かるものであり，開発現場の技術者にとって有益な情報である．しかし，定理証明では，命題を証明できた場合はともかく，証明できなかった場合には何も情報が得られない場合がある．命題が成り立たたないからといって反例が得られるとは限らない．このような道具立てを現状でのソフトウェア開発現場でもちいるには，より一層詳しい説明を技術者に提供する必要がある．

まとめ

フィールドワークを通して，先端技術に関する知見と技能を共同研究先に移転することが，フィールドワークに期待される効果の１つであることはいうまでもない．そのためには，研究開始時はともかく，開始後一定の期間が経過した後には共同研究相手の技術者がモデル検査などの先端技術を使って検証作業に携わることが必要である．そのためにはもちろん，技術者に技術を教えなければならない．要するに，フィールドワークは人材養成活動を必然的にうみだすものであり，人材養成と切り離して考えることはできない．AIST/CVS でも，モデル検査の実用研究において，技術者養成の必要が生じたため，それを独立させて，モデル検査に限らず，数理的技法一般における人材養成の事業をはじめている [1)]．

フィールドワークに期待される効果のもう１つのものは，この経験から科学研究の新しい方向をうみだすことである．本稿で紹介した例だけでも，図示記法というグラフィックな記述法の研究，環境ドライバの概念の定式化，故障解析の枠組みなど，今後の科学研究の方向への示唆がいくつかある．学術研究が象牙の塔にこもって閉塞状況に陥ることを避ける意味からも，フィールドワークを重視していきたいと我々は考えている．

最後に，本稿で紹介したフィールドワークにおいて共同研究の相手をつとめてくださった矢崎総業(株)および関連会社，(株) イシダおよび事例 (2) における匿名の企業に，共同研究を遂行していただいたこと，および本稿の発表を快諾いただいたことに対して厚くお礼申し上げます．これらの企業の協力がなければ，フィールドワークは成り立ちませんでした．また，産業技術総合研究所側のメンバとして，Reynald Affeldt，池上大介，尾崎弘幸，小池憲史，齋藤正也，高木浩光，中野昌弘，松本利雅，山形頼之，山下伸夫，吉田聡の諸氏が本稿で紹介した共同研究計画に参加されました．本稿準備にあたってさまざまな形でご協力いただいたことを感謝します．

参考文献

1) システム検証研究センター：4 日で学ぶモデル検査初級編，エヌ・ティー・エス (2006).
2) 小池憲史，吉田　聡，大崎人士：LTL モデル検査の為の図示記法，第 14 回ソフトウェア工学の基礎ワークショップ（FOSE2007），下関，日本ソフトウェア科学会 (Nov. 2007).
3) 吉田　聡，竹内　泉，小池憲史，大崎人士：図示記法表現と LTL 論理式，第 10 回プログラミングおよびプログラミング言語ワークショップ（PPL2008），仙台，日本ソフトウェア科学会 (Mar. 2008).
4) 高井利憲，古橋隆宏，尾崎弘幸，大崎人士：環境ドライバを用いたモデル検査による検証事例，第 4 回システム検証の科学技術シンポジウム，名古屋，日本ソフトウェア科学会 (Nov. 2007).
5) 河本孝久，小池憲史，古橋隆宏，鈴木伸一：周期タスク型モデル検査法と車載組込みシステムへの適用事例，組込みシステムシンポジウム（ESS2007），東京，情報処理学会 (2007).
6) 高井利憲，吉田　聡：アセンブラプログラムのモデル検査による検証事例，第 5 回ディペンダブルシステムワークショップ（DSW2007），函館，日本ソフトウェア科学会 (July 2007).
7) 高井利憲，吉田　聡：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，第 4 回システム検証の科学技術シンポジウム，名古屋，日本ソフトウェア科学会 (Nov. 2007).
8) Clarke, E. M., Grumberg, O. and Peled, D. : Model Checking, MIT Press (1999).
9) 吉田　聡，山形頼之：ソフトウェア更新システムプロトコルの BAN Logic による安全性検証（Preliminary Version），算譜意味論研究速報，PS-2007-006 (June 2007).
10) 山形頼之，斎藤正也：ソフトウェア更新システムのモデル検査によるセキュリティ，算譜意味論研究速報，PS-2007-008 (July 2007).
11) 斎藤正也，高井利憲，池上大介：Java の例外処理の SPIN による検証，第三回システム検証の科学技術シンポジウム，豊中 (Oct. 2006).
12) 篠崎孝一，太田　弘，早水公二，星野光勇，今村哲典，吉田雅昭：モデル検査の実用化課題と支援ソフトウェアの開発，第三回システム検証の科学技術シンポジウム，豊中 (Nov. 2006).
13) 栗田太郎，太田豊一，中津川泰正：モバイル FeliCa IC チップ開発における形式仕様記述手法導入の効果と課題，第 25 回 Software Symposium 2005 (June 2005).

（平成 20 年 3 月 31 日受付）

木下佳樹（正会員）
yoshiki@m.aist.go.jp
平成元年東京大学大学院理学系研究科博士課程情報科学専攻修了．理学博士（情報科学）．テキサスインスツルメンツ，電子技術総合研究所を経て，現在（独）産業技術総合研究所システム検証研究センター研究センター長．

高井利憲（正会員）
t-takai@aist.go.jp
平成 8 年九州工業大学情報工学部知能情報工学科卒業．平成 13 年奈良先端科学技術大学院大学博士後期課程単位取得認定退学．科学技術振興機構 CREST 研究員などを経て現在産総研システム検証研究センター研究員．博士（工学）．

大崎人士（正会員）
ohsaki@ni.aist.go.jp
筑波大学大学院工学研究科修了．博士（工学）．2000 年旧電子技術総合研究所入所，2001 年改組により産業技術総合研究所に異動．ほかに，さきがけ研究「機能と構成」領域（JST）の研究員（兼任）や，招聘研究員（イリノイ大学，エコール・ノルマル・シュペリエール・カショーン校他）の研究歴がある．文部科学大臣表彰若手科学賞受賞（2006 年 4 月）．計算論，特にツリーオートマトンと書換系（かきかえけい）の研究に興味を持つ．