National Institute of
Advanced Industrial Science
and Technology
AIST

AIST-PS-2009-009

MCBOK2008: ソフトウェア開発のための モデル検査知識体系

西原秀明 [1], 青木利晃 [2], 粂野文洋 [3,4],
篠崎孝一 [5], 田口研治 [3], 早水公二 [6]

[1] 産業技術総合研究所 システム検証研究センター
[2] 北陸先端科学技術大学院大学 情報科学研究科
[3] 国立情報学研究所 先端ソフトウェア工学・国際研究センター
[4] 三菱総合研究所
[5] 関西電力 電力技術研究所
[6] メルコ・パワー・システムズ

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

MCBOK2008: ソフトウェア開発のためのモデル検査知識体系

西原秀明[†1] 青木利晃[†2] 粂野文洋[†3,†6]
篠崎孝一[†4] 田口研治[†3] 早水公二[†5]

機能安全やセキュリティ評価基準において，形式手法の採用が強く推奨されているなど，システムの安全性を保証する分野において，形式的検証技術の利用が広がりつつある．その中でもモデル検査は有望な技術として認められつつある．モデル検査の習得環境を整備し，普及を促進することを目的として，産学官の組織が連携し，ソフトウェア開発にモデル検査を適用する際の知識を MCBOK 2008 (Model Checking Body Of Knowledge) として体系立ててまとめた．本論文では MCBOK 2008 の概要と，想定される MCBOK の用途について述べる．また，MCBOK 2008 を作成する際にとった手法，得られた知見について述べる．

MCBOK2008: Model Checking Body Of Knowledge for Software Development

Hideaki Nishihara ,[†1] Toshiaki Aoki ,[†2] Fumihiro Kumeno ,[†3,†6]
Koichi Sinozaki ,[†4] Kenji Taguchi [†3] and Koji Hayamizu[†5]

Formal verification is now a well-recognized method in system development, as a method to improve safety and dependability property of systems. In particular, model checking is regarded as a feasible formal verification methods. To build a good environment to learn model checking, and to make it spread in industry, authors from academia, industry, and a public institute arrange knowledge about model checking to Model Checking Body Of Knowledge (MCBOK 2008). In this article, MCBOK 2008 is reviewed and its applications are shown.

1. 導　　入

情報処理システムの普遍化，複雑化によって，システムに要求される信頼性はますます高くなってきている．製品に組込まれて世に出たシステムにバグが発見されて社会に影響を与えた例は近年特に散見されるし，開発側企業でも品質の確保・向上を重要な課題として認識している[13)]．国際規格である機能安全規格 (IEC61508)[4)] やセキュリティ評価基準 (ISO/IEC15408)[5)] などでシステムの安全さが規定されたのは上記の状況を反映したものであるといえよう．

この状況において，近年注目されているのが形式手法である．特にモデル検査は人間が見落としがちな想定外の振る舞いを全数探索によって発見することができ，強く期待されている．近年では産業界一般における認知度も高まり，国内でもシステム開発における本格的な導入が進み，多方面の分野における適用事例 や企業により開発されたツール が発表されるなど注目されている．さらに，モデル検査を科目として持つ大学のカリキュラムや人材育成プログラムも増えてきているし，モデル検査を特色としてあげるコンサルテーション企業も存在する．

ところが，モデル検査に関する教育の整備はまだ十分とはいえない．モデル検査は複数の理論的基盤を持つので，それを反映して検査ツールも多様であるし，技術の汎用性から適用領域も幅広い．よってモデル検査全体をカバーするカリキュラムを策定しても抽象的

†1 産業技術総合研究所 システム検証研究センター
Research Center for Verification and Semantics, National Institute of Advanced Industrial Science and Technology(AIST)
†2 北陸先端科学技術大学院大学 情報科学研究科
School of Information Science, Japan Advanced Institute of Science and Technology
†3 国立情報学研究所 先端ソフトウェア工学・国際研究センター
Grace Center, Information Systems Archtecture Research Division, National Institute of Informatics
†4 関西電力 電力技術研究所
The Kansai Electric Power Co.
†5 メルコ・パワー・システムズ
Melco Power Systems Co.
†6 三菱総合研究所
Mitsubishi Research Institute

或いは量が膨大になってしまってシステム開発への導入という最終目標にそぐわないものになってしまう．目的，前提知識などの状況に応じて内容を取捨選択し，カリキュラムを策定するためのツールが求められている．

著者らは産，学，官それぞれの立場から技術者向けモデル検査の教育・普及を進めてきたが，産業界で高まりつつある需要を受け止め，更に普及を推進するためには教育内容の統一的な基礎付けが必要だという認識に至った[6),14)]．つまり，ソフトウェア開発にモデル検査を適用するという観点からモデル検査の知識を体系化することで，前述したモデル検査の習得と普及に対する障壁を取り除くことが出来る．

著者らの活動の初期段階でこのようなモデル検査教育の基礎となるものを調査したが，要求をみたすものを見つけることができなかった．ソフトウェア工学の教育に関する資料 (SWEBOK[1)]，SE2004[8)], J07[12)] など) においても，形式手法がトピック名として現れている程度で，モデル検査とその知識については殆ど記載がない．

そこで，著者ら自身でモデル検査の知識を体系化し，教育の基礎付けを与えることにした．その成果である知識体系をソフトウェア開発のためのモデル検査知識体系 (MCBOK 2008) と呼ぶことにする．

MCBOK 2008 は「モデル検査のプロセス」,「モデル検査の理論」,「モデル検査ツール」,「モデル検査の適用対象」の四つの領域を持ち，モデル検査の知識が存在する広い範囲から知識項目を収集して体系化している．各領域は段階的に副領域に分割され，その中に「有限オートマトン」「内部モデル/外部モデルの設計」「NuSMV」といった知識項目が分類されている．このように各知識項目は十分に具体的で応用しやすい形になっている．

MCBOK 2008 の作成にあたっては，モデル検査に関する学術的な知見を持つ大学・研究所と，実践的な知見や需要を持つ企業とが共同で作業を進めた．それにより，理論と実践双方の知識を偏り無くまとめた，ソフトウェア開発の場で有益である知識体系となった．

MCBOK 2008 はモデル検査カリキュラムの基礎的な資料として機能する．第 5 節で述べるように，著者らがこれまで進めてきた教育活動のカリキュラムとの対応づけを考えることで，カリキュラムの扱う内容を顕にして特徴付ける．新たにカリキュラムを策定する際にも，到達目標に合った教育する知識の選択を支援する．その他，技術認定の枠組み構築や，コンサルテーションなど，モデル検査の関係する幅広い活動の基礎資料として機能することを期待している．

本論文では，MCBOK 2008 とその開発，用途について述べる．第 2 節でモデル検査について，第 3 節で BOK について一般的な立場から解説する．第 4 節で，著者らが開発した MCBOK 2008 について説明する．知識の領域の分割や MCBOK 2008 に特有の事情，策定の方法論に属する事柄を併せてこの節で述べる．第 5 節で，MCBOK 2008 の使い方を幾つか紹介する．既存のカリキュラムから MCBOK 2008 への対応付けを例示し，その特徴づけを行うほか，想定される用途について説明する．最後に第 6 節で MCBOK の今後の展望と課題について述べる．付録として，MCBOK 2008 を末尾に掲載した．

2. モデル検査

モデル検査は形式手法に分類される検証技術の一つである．オートマトンとしてシステムをモデル化し，また検査項目を時相論理式として記述し，この時相論理式がモデル上で成立するかどうかを全数探索によって検査する．LTL, CTL などの各種の論理体系，オートマトン，状態遷移系など各種のモデル記述体系が存在し，その状況を反映して数多くのモデル検査ツールが開発されている．

検査対象を一旦モデル化することから，設計などの上流工程から適用することができ，モデル検査の適用によってシステム開発時の手戻りを減らすことができる．また，全数探索によって，時相論理式がモデル上で成立しない場合のモデルの振る舞いを反例として出力するので，モデル検査はモデルやシステムの解析を支援する．

モデル検査は，組込みシステムに代表されるような複数の小さなシステムが並行動作するシステムの検証と相性がよく，人間が見落としがちな設計・実装の微妙な不備から来る想定外の振る舞いを発見することができる．また形式手法の中であまり前提知識を必要とせず，技術者が比較的容易に習得することができる．従来，発電所制御や電話交換機制御などのインフラや航空機の制御など極めて高い信頼性が要求されるシステムで適用されていたモデル検査であるが，計算機資源の量的向上や情報処理システムの信頼性が重視される社会状況から，現在では多方面の分野において適用されている．機能安全規格 (IEC61508)[4)] やセキュリティ評価基準 (ISO/IEC15408)[5)] では，システムにおけるある水準の信頼性を保証するために，開発時に形式手法による検証を行うことを強く推奨している．

3. BOK

ある分野における知識を体系化してまとめたものを知識体系 (Body Of Knowledge) と呼び，BOK と略記する．知識には用語・概念のような理論に属するものも含まれるし，実践の際にノウハウとして適用されるようなものも含まれる．ソフトウェア開発に関連する分野では，ソフトウェア工学知識体系 SWEBOK[1]，プロジェクトマネジメント知識体系 PMBOK[7] やソフトウェア品質知識体系 SQuBOK[15] などがあげられる．情報処理学会による「情報専門学科カリキュラム標準 J07」[12] では領域ごとにカリキュラムの土台として BOK を定めている．

BOK は対象領域における知識の構造を可視化し，それは多くの場合に教育・人材育成と関連して利用される．先にあげたようにカリキュラム標準 J07 は領域ごとの知識体系をベースに内容を決定している．米国の学部生向けソフトウェア工学カリキュラム SE2004[8] でも SWEBOK，PMBOK，その他関連分野における既存の BOK の影響の下に独自の知識体系 SEEK (Software Engineering Education Knowledge) を策定し，その上にカリキュラムを構築した．また，SQuBOK[15] はソフトウェア品質技術者認定試験で唯一の参考書としてあげられており，技術認定の基盤として使われている．人材育成以外では，SWEBOK の序文に ‘industrial decision’ の基盤となることが目的の一つとしてあげられている．

多くの BOK では対象領域に関する知識を三段階から五段階程度の樹形図の上に配置することで構造を可視化している．BOK に求められるものは，本質的にこの樹形図だけであって，そこに現れる知識の解説や参照文献などは「ガイド」として別に扱うことが多い．

4. MCBOK2008 の開発

付録にソフトウェア開発のためのモデル検査知識体系 (MCBOK2008) を掲載した．

MCBOK2008 ではモデル検査の知識を「モデル検査のプロセス」「モデル検査の理論」「モデル検査ツール」「モデル検査の適用対象」の四つの知識領域 (Knowledge Area : KA) に分類している．さらに各領域を副領域に詳細化し，最大で四階層に全体の知識をまとめている．

ここで，MCBOK 2008 はモデル検査の知識を完全に網羅したり，モデル検査が関係する範囲を規定するものではないことを注意しておく．MCBOK 2008 はソフトウェア開発という観点から知識をまとめたものであり，他の観点から内容が偏っているように見えても不思議はない．

4.1 開発のポイント

各領域について説明を加える前に，MCBOK 2008 の開発について述べる．まず，BOK には一般的な定義がなく，従って開発方法論というものも確立されていない．しかし，幾つかの BOK は開発過程を文書化しており (例えば Guide to SWEBOK には SWEBOK の開発方法について述べた章がある)，開発に関する知見・経験が述べられている．

MCBOK 2008 の開発に際しても既存の BOK の方法論を参考にした．しかしモデル検査には以下のように事情もあり，そのまま通用するわけではない．

- 対象とする範囲の差．SWEBOK においては，モデル検査という用語は第四階層の説明文で初めて現れており，J07 でも似たような状況にある．MCBOK 2008 は SWEBOK や J07 に比べると非常に狭い領域を対象としている．そのため，具体的な知識項目まで扱うことができ，即時応用可能な知識体系となったが，一方でその具体性ゆえに項目の扱いに意見の相違が見られることもあった．
- 今まさに普及途上にあること．既存の BOK が対象としている領域に比べて，モデル検査の知識としてまとめられ，公開されている論文や書籍は少ない．知識領域の設定，項目の収集においても，「文献はないが，知識が存在して然るべき」と判断して進めざるを得ない場合があった．このような箇所は妥当性，有用性の観点から特に注意深く評価しなければならない．

MCBOK 2008 の開発は，以下のように項目の拾い出し，項目の取捨選択と体系化，評価と改善，の三つの工程で進められた．但し三つの工程が明確に分かれていたわけではない．開発の初期段階から項目を木構造に並べたものを試験的につくっており，第一の工程，第二の工程のベースとなっている．

- 知識項目の拾い出し．モデル検査における知識を調査し，BOK に採用する知識の候補を収集する．この段階では項目の取りこぼしを恐れてソフトウェア開発という視点を忘れ，モデル検査全般に関する知識を調査した．出版されているモデル検査のテキスト，著者が使用しているカリキュラムを主な調査範囲とし，KA 1 と KA 4 については国内で発表された論文，記事，報告書，産総研の検証事例データベース[10] を調査範囲とした．モデル検査全般の知識は多岐に渡り，またその深さ

も様々である．検討を重ねても採用する項目の数が収束しない部分もあったが，後工程の体系化によって知識項目の位置づけが明確になることも予想され，採否に関する議論は次の工程に一部持ち越された．

- 項目の取捨選択と体系化．収集した知識を分類，体系化する．収集した知識をソフトウェア開発という視点から整理した．開発初期には，テスト，静的解析や国際規格を扱う「モデル検査関連項目」という五番目の知識領域を設定していた．しかし，直接モデル検査に関する知識があげられるかどうか疑問があること，モデル検査に無関係な知識で知識体系が発散する可能性があることから領域ごと取り除いた．
- 成果物の評価と改善．後の第 5 節で詳しく述べるように，MCBOK 2008 はカリキュラム策定・評価，モデル検査技術認定，保有する技術の可視化，モデル検査適用指針決定の各場合での基礎資料となることを想定している．これらの用途に沿った形で MCBOK 2008 を評価することが望ましい．しかし，カリキュラム策定と技術認定という点からの評価は長期的なものになりがちでカリキュラムの評価からくる間接的なものになりやすい．
  今回はモデル検査の適用経験がある少数の技術者に聞き取り調査の形で評価を受けた．各知識項目について，(a) その知識を整理した形で持っているか (b)(知識として整理していなくとも) その知識に相当することをソフトウェア開発の場で実施しているか (c) その知識に関心があるか，の三点について質問し，回答を得た．但し,「モデル検査の理論 (KA 2)」については直接質問はしていない．結果として，MCBOK 2008 にあげた知識項目の殆どの部分で，知識またはノウハウを持っているという回答が得られた．今後，広い範囲からの更なる評価が求められるが，MCBOK 2008 は産業界の実態や関心と大きくかけ離れたものではないといえる．

4.2 モデル検査のプロセス (KA 1)

KA 1. ではモデル検査をソフトウェア開発に適用する際の知識を体系化している．現在モデル検査が普及途上にあるということから，この知識領域に関する文献はまだ少なく，公知の知識を収集して整理するという方法はうまく機能しないおそれがある．領域を偏り無く適切に分割し知識を拾い出すために幾つかの適用事例を分析し，知識が存在する箇所を特定した．

KA 1.1 では目的と工程によってモデル検査の適用に関する知識を整理している．例えば，上流工程のうちに設計の不具合を発見するという適用形態もあれば，実装から不具合の原因 (不具合現象自身は既知であってもその原因が特定できないことはよくある) を求めるという適用形態もある．

KA 1.2 「モデル検査の適用手順」にはモデル検査を適用するというプロセス自体についての知識を整理している．検査範囲の特定，モデルの抽象度決定，外部環境の構築，モデル検査で検査できる性質，ツールの実行などが含まれている．

モデル検査を開発に適用するに当たり，そのコストに関する知識は重要な意味を持つ．KA 1.3 「モデル検査のコスト」では，導入段階，導入後本格的な運用段階にかかるコスト，そして効果が知識項目として挙げられている．

KA 1.4 「モデル検査の実施体制」は開発者自身がモデル検査を使って検査を行うのか，それとも第三者検証のように専門家が検査するかについての知識が項目としてあげられている．

4.3 モデル検査の理論 (KA 2)

KA 2 は理論的基礎に関する知識を体系化した領域である．ツールが十分に発達した段階では，理論を意識しなくてもモデル検査の適用は可能である．しかし現在の段階ではモデルや論理式の手入力がまだ主流であるし，背後の理論を念頭においてモデルや検査式を作成し検査プロセスを進めることも重要である．

この領域は教科書，論文など数多くの文献が蓄積されている．モデル検査の標準の教科書である[2),3)]，著者の既存のカリキュラム[9),11),14)]，テキストから項目を収集した．

KA 2.1「計算モデル」にはモデルを記述するための枠組みを整理した．多くのモデル検査ツールでは有限オートマトン，またはそれに類する各種の構造を使ってモデルを記述する．個々の計算モデルについて，それを基盤とする検査ツールがあり，ソフトウェア開発における適用例があるものを選んで知識項目として採用した．

KA 2.2 「時相論理」には検査式を記述する論理体系について整理した．現在モデル検査で使われている論理体系は LTL と CTL を基にしている．それぞれの意味論と決定可能性，表現力をここで扱う．

KA 2.3 「モデルの縮小手法」は状態爆発問題の回避方法に関する知識を整理した．モデル化の対象の分析によってモデル化の範囲を縮めることで縮小する方法もあり，一旦モデル化したものを機械的に縮小する方法もある．縮小の前後を比較し正当性を示す手段も

含む.

KA 2.4「モデル検査の原理」では，モデル上での検査式の妥当性を検査するアルゴリズムの知識について整理した．ある意味個々の検査ツールと強い関連を持つ知識であるが，アルゴリズム自身は純粋に理論的な知識であり具体的な実装とも区別できる．よって「モデル検査の理論」の知識領域に配置している．

4.4 モデル検査ツール (KA 3)

KA 3 はモデル検査ツールに関する知識を体系化した領域である．ソフトウェア開発における適用例があり，動作原理についての文献が存在しているものを採用した．ツールにはモデル検査そのものを行う (C.f. KA 2.4) ツールと，その利用を支援するツールがあり，この観点から副領域を分割した．

KA 3.1 はモデル検査アルゴリズムを実行するツールを整理した領域である．モデル検査ツールは個々に基盤となる理論，入出力の形式，検査規模の限界，検査できる性質が異なり，MCBOK でも 6 個の領域に分かれている．一つ目の項目の「基本モデル検査ツール」は Spin, Cadense SMV, NuSMV といった，現在主流と呼ばれているツールを含んでいる.「基本」という形容は適当でないかもしれないが，他に良案もなく，便宜的に「基本モデル検査ツール」と呼んでいる．

KA 3.2 はモデル検査アルゴリズムを実行するものではないが，検査作業を支援するツールを整理している．XSpin のようなフロントエンドとして機能するツールは「モデル検査ツールの使用支援ツール」に，UML チェッカーのようなツールは「設計検査支援ツール」に分類している．

4.5 モデル検査の適用対象 (KA 4)

「モデル検査の適用対象」は適用事例を分類したものである．モデル検査は理論的な適用範囲は広く，殆ど全てのシステムを適用対象とすることができるが，適用効果が高い分野とそうでない分野がある．また，未だモデル検査が日常的に使われているとは言いがたい現状にあって，適用例を整理してまとめておくことには MCBOK の目的からも価値があるとしてこの領域を設定した．事例の収集は国内の論文，報告書，雑誌記事など公刊されているもの，産総研の事例データベース[10] に拠った．

KA 4.1 はアプリケーションシステムへの適用を整理した．web システムや業務系のシステムでは，状態遷移をベースに設計されることもあり，モデル検査との相性はよい．

KA 4.2 ではミドルウェアへの適用を整理した．ミドルウェアはアプリケーションシステムの土台となり，システム全体に影響を及ぼすので高い信頼性が求められる．いわゆる刺激応答型システムでもあり並行性もあり，モデル検査の特徴が生きる領域である．

KA 4.3 ではネットワークへの適用を整理した．特に通信プロトコルの検証は，歴史的にモデル検査が盛んに適用されてきた領域である．

KA 4.4 では，組込みシステムへの適用を整理した．組込みの分野は近年盛んに研究開発が進んでおり，モデル検査の適用事例も散見される．

5. 学習・普及のツールとしての MCBOK

MCBOK 2008 の目的はモデル検査における知識の構造を可視化し，産業界 (主にソフトウェア開発分野) へのモデル検査の普及を推進することである．この節で述べるように，MCBOK 2008 はモデル検査の教育，普及，適用の際のツールとして有効に機能する．

5.1 カリキュラムの基礎付け

一般に，何かの教育を行う際には，その目的と到達目標を明確にし，それに合わせて教育内容，順序や時間配分，前提知識などを決めていかなければならない．

モデル検査に関しても事情は同じであるが，ソフトウェア開発に適用するという視点からみると，目的と到達目標に広い幅があることが予想される (4.2 節, 4.5 節にあげた知識項目はこの状況を反映している．). 従って教育内容や教育の順序その他も多彩なものが考えられる．例えば，開発プロジェクトにモデル検査を導入するかどうかを判断するリーダーと，検証しながら設計を進めたいエンジニアと，不具合の原因をモデル検査で発見したいエンジニアとでは持っているべき知識に違いがあるし，当然開発対象の属する分野によっても異なる．現在，モデル検査に関するテキストが何点か出版されてはいるが，読者の多様な目的と目標に対応するには不十分である．

そこで，MCBOK 2008 がモデル検査カリキュラム策定・評価の基礎資料として機能する．策定の際には，目的に応じて各知識領域から必要な知識項目を選択し，次いで扱いの重み，知識の依存関係，時間数などを考慮してカリキュラムとして確定する．評価の際は逆にカリキュラムの内容と MCBOK 2008 の各知識とを対応づければよい．

モデル検査の細部を知る必要はないが，モデル検査の実績と可能性，プロセスについて知る必要のある開発リーダー向けには「モデル検査のプロセス (KA 1)」「モデル検査の適用領域 (KA 4)」の知識を多く含むように項目を選択してカリキュラムを作成する．KA1, KA4 の知識は抽象概念や理論的な知識と深い関連は

表 1 産総研モデル検査初級カリキュラムから MCBOK 2008 へのマッピング
Table 1 Mapping from AIST's curriculum to MCBOK 2008

カリキュラム項目	対応する知識領域
モデル検査とは	
状態, 遷移, 次の瞬間, 非決定的/決定的	1.2(4),2.1(1)
安全性, 活性	1.2(2)(6)
モデル検査の基礎	
状態と遷移を定めて状態遷移系を書く	1.2(1)(4)
検査する性質:正しい性質/反例のある性質	1.2(2)
遷移系を目でみて検査	1.2(7)
ツールによるモデル検査	1.2(5)(6)(7)(8)
検査式の記述	
直列回路, 並列回路, And/Or の導入	1.2(6)
Until operator	1.2(6)
並行システムと排他制御	
並行システム/セマフォ/Critical Section	1.2(4)(5), 2.1(1), 4.2
検査:同時に CS に入らない	1.2(2)
検査:各プロセスとも CS に入ることが可能	1.2(2)
公平性の問題	2.1(1)
LTL	
パス, パス上の真偽	2.2(1)
様相記号	2.2(1)
意味論	2.2(1)
LTL 式を書く演習	1.2(2)(6),2,2(1)
ソースコード検査	
簡単な C プログラムのモデル化	1.2(4)(5), 4.1
テスト技法とモデル検査の違い	-
演習:自動販売機	1.2(4)(5)(6)(7)(8), 4.1

なく，カリキュラムの受講者に課す前提知識は一般的なソフトウェア工学と経験があれば十分だろう．一方，実際に検証を行うエンジニア向けには「モデル検査のプロセス (KA 1)」「モデル検査ツール (KA 3)」に属する知識を多く含むカリキュラムを作成する．エキスパート育成という要素があるのならば「モデル検査の理論 (KA 2)」の項目をカリキュラムに含めるべきだろう．

既存のカリキュラムを評価する際にも MCBOK 2008 は有効に機能する．**表 1** は産総研のモデル検査初級のカリキュラム[14] について，各項目の MCBOK 2008 の対応する知識領域を表したものである．このカリキュラムには「モデル検査のプロセス (KA 1)」の知識が多く扱われており，モデル検査の適用のしかたに興味を持つ学習者に適していることがわかる．

5.2 技術認定

技術者が身につけた知識や技能を明らかにし,「何ができて，何ができないか」を正確に把握することは，本人にとっても周囲にとっても重要なことである．教育活動の際にも，事後に内容を確認し，設定した到達目標の達成度を評価する仕組みがあると動機付けにもなり効果が高い．

そのための一つの方法として，試験の成績など一定の条件を満たした者に対してその技能を認定する，ということがある．その際，認定の仕組み自体に信頼性が求められる．特にモデル検査のように普及途上にある技術の場合，認定制度の確立は技術の普及に貢献すると思われるが，一方で認定する内容を明らかにし,「何ができるか」ということを周知して認定制度の価値を高める必要があるだろう．

MCBOK 2008 は上記のような認定の基礎となることができる．

5.3 保有する知識の可視化

個人が自分の持つ技術の程度を知るツールとしても MCBOK 2008 は有効に働く．モデル検査に関して幾らかの知識を持つ技術者が，MCBOK 2008 に挙げられている個々の知識について，

- モデル検査の適用時に，その知識を意識しているか，
- その知識を自分なりに知識として整理して使っているか，

を確認することで，その技術者が保持する知識や適用時に意識していることを明確にできる．同様に不足している知識，その時点では必要でない知識も明確になり，将来の学習計画を立てる際にも有用である．

5.4 モデル検査の適用の指針

システム開発プロセスへのモデル検査導入を検討する際のツールとして MCBOK 2008 は機能する．開発プロジェクトにおいて，開発対象の種類や特徴によって，また使用する他の開発技術によって，モデル検査をどの部分にどの程度適用するか違いが出てくる．MCBOK 2008 の「モデル検査のプロセス (KA 1)」を参照することで，モデル検査の適用工程に関する知識が明らかになり，開発工程の適切な部分でモデル検査による検証を行えるようになる．また,「モデル検査ツールの選定 (KA 1.2(3))」と「モデル検査のツール (KA 3)」を併せて参照することで，問題に即したツールを選択し検証を進めるための判断材料が得られる．

6. 今後の展開

本論文でソフトウェア開発のためのモデル検査知識体系 MCBOK 2008 を提案し，その開発方法と用途について述べた．これを受けて次の計画が幾つかあがっている．

まずは MCBOK 2008 を用いてモデル検査の産業界への普及を推進することである．第 5 節で述べたよ

うに，MCBOK 2008 はモデル検査カリキュラムの作成・評価，技術認定を中心とした保有する技術の可視化，ソフトウェア開発における適用の際の判断の基礎資料となる．既存カリキュラムの MCBOK 2008 へのマッピング，技術認定の枠組み構築などにより産業界におけるモデル検査の認知度が高まり，普及が加速していくと期待している．

次に MCBOK 2008 の評価を続け，知識体系としての質をあげていくことである．今回，技術者からの聞き取りという形で MCBOK 2008 の評価を得た．しかし第 4.1 節でも述べたように，想定する MCBOK 2008 の用途に沿った形で広い範囲から外部からの評価を得るべきである．また，BOK の開発という観点からは，今回属人的な工程が殆どで，改善の余地が多々ある．今後開発手法を見直し，系統的な BOK の開発と改良を進めたい．更に，得られた系統的 BOK 開発手法をもとに，形式手法の他の分野についても BOK を開発したいと考えている．

謝辞　産業技術総合研究所の高村博紀氏，吉田聡氏，渡邊宏氏には MCBOK 2008 の作成段階でご協力頂いた．また三菱総合研究所の石黒正揮氏と富士ソフト株式会社の小池隆氏からは MCBOK 2008 の評価にご協力頂いた．謹んで感謝の意を表する．

参 考 文 献

1) Abran, A., Moore, J. W., Bourque, P. and Dupuis, R.: *Guide to the Software Engineering Body of Knowledge 2004 Version SWEBOK*, IEEE (2004).
2) Clarke, E. M., Grumberg, O. and Peled, D. A.: *Model Checking*, The MIT Press (2000).
3) Holzmann, G. J.: *The SPIN model checker: Primer and reference manual*, Addison Wesley (2004).
4) IEC61508: *Functional safety of electrical/ electronic/ programmable electronic safety-related systems*, Bureau Central de la Commission Electrotechnique International (2000).
5) ISO/IEC15408: *Information technology - Security techniques - Evaluation criteria for IT security - Part1, Part2 and Part3*, ISO/IEC (2005).
6) Nishihara, H., Shinozaki, K., Hayamizu, K., Aoki, T., Taguchi, K. and Kumeno, F.: *Model Checking Education for Software Engineers in Japan*, SIGCSE bulletin inroads (to appear).
7) Project Management Institute: *Guide to the Project Management Body of Knowledge*, PMI (2000).
8) The Joint Task Force on Computing Curricula, IEEE Computer Society, Association for Computing Machinery: *Software Engineering 2004, Curriculum Guidelines for Undergraduate Degree Programs in Software Engineering* (2004).
9) 産業技術総合研究所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).
10) 産業技術総合研究所システム検証研究センター: システム検証の事例報告集 2008 年度版, 算譜科学研究速報 aist-ps-2009-004, 産業技術総合研究所 (2009).
11) 吉岡信和, 青木利晃, 田原康之: SPIN による設計モデル検証–モデル検査の実践ソフトウェア検証, 近代科学社 (2008).
12) 情報処理学会情報処理教育委員会, J07 プロジェクト連絡委員会: 情報専門学科におけるカリキュラム標準 J07.
13) 経済産業省 商務情報政策局 情報政策ユニット情報処理振興課: 2008 年度版組込みソフトウェア産業実態調査報告書.
14) 青木利晃, 粂野文洋, 木下佳樹, 篠崎孝一, 高木理, 高村博紀, 田口研治, 中原早生, 西原秀明, 早水公二, 本位田真一, 渡邊宏: モデル検査の教育プログラム構築に向けて, 算譜科学研究速報 aist-ps-2008-012, 産業技術総合研究所 (2008).
15) 日本科学技術連盟, 日本品質管理学会: ソフトウェア品質知識体系ガイド.

付録

MCBOK 2008

KA1

モデル検査のプロセス

1.1 モデル検査の適用方法
- 設計検証プロセス
- 開発ツール一体型適用プロセス
- ソースコード検証適用プロセス
- デバッグ適用プロセス
- アドホックな適用

1.2 モデル検査の適用手順

検査対象の選定
- 適用工程／詳細化レベルによる選定
  （仕様／設計／コード）
- システムの特徴による選定
  （状態遷移系／並行動作／通信）

検査項目の設定
- 検査できる性質（到達可能性／活性）
- 検査の観点（仕様／固有知識）の獲得
- 検査項目の具体化
- モデル動作確認のための検査項目

モデル検査ツールの選定
- モデル／検査内容による選定
- モデルの複雑さによる選定

モデル設計
- モデル化範囲／レベルの決定
- 内部モデル／外部モデル
- 非決定性・公平性
- 検査項目との整合性

モデル実装
- 専用プログラム記述
- GUI入力
- 開発用言語による入力

検査項目の記述
- 時相論理式による記述
- プロパティパターン
- アサーション記述
- 観測変数のモデル化

モデル検査ツールの実行
- 実行順序（モデル確認から重要な検査へ）
- 状態爆発への対応（打ち切り、モデル変更）
- 繰り返し実行

反例解析
- トレース分析（停止／ループ）
- シミュレーション実行
- 検査項目／モデルの不具合修正
- 検査項目／モデルの変更
- 対策要否の検討

1.3 モデル検査のコスト
- 導入（教育）コスト
- 作業コスト
- 効果

1.4 モデル検査の実施体制
- 専門チーム
- 設計者／テスト技術者

KA2

モデル検査の理論

2.1 計算モデル

オートマトン
- 有限オートマトン
- 無限オートマトン
- 時間オートマトン
- ωオートマトン
- 確率オートマトン
- プッシュダウンオートマトン
- ハイブリッドオートマトン
- 非決定性
- 公平性

プロセス代数
- CCS
- CSP
- π計算

項書き換え系
- 項書き換え系

2.2 時相論理

LTL
- LTLの Kripke 意味論
- 決定可能性と決定手続き

CTL
- CTLの意味論
- 決定可能性と決定手続き

時相論理の表現力
- 実時間論理
- CTL＊
- 様相μ計算

2.3 モデルの縮小手法

モデル間の関係
- 抽象解釈
- Cone of Influence Reduction
- Partial Order Reduction

モデルの最適化
- 抽象化
- スライシング

2.4 モデル検査の原理

記号モデル検査

On the Fly モデル検査

有界モデル検査

無限有界モデル検査

KA3

モデル検査ツール

3.1 モデル検査ツールの種類

基本モデル検査ツール
- Spin
- Cadence SMV
- NuSMV

プロセス代数のモデル検査ツール
- LTSA
- FDR
- Mobility Workbench

無限状態モデル検査ツール
- SAL
- Maude

実時間モデル検査ツール
- UPPAAL
- KRONOS

確率モデル検査ツール
- PRISM

ハイブリッドシステムモデル検査ツール
- HYTECH

モダンモデル検査ツール
- BLAST
- Java Path Finder
- Bandera
- Varvel
- SLAM

3.2 モデル検査支援ツール

設計検査支援ツール
- HUGO
- vUML
- charmy
- UMLチェッカー

Eデル検査ツールの使用支援ツール
- Xspin
- Lambda Trace

プログラム検査支援ツール
- FeaVar(MODEX)

KA4

モデル検査の適用対象

4.1 アプリケーションシステム
- web アプリケーション
- グループウェア
- 交通管理システム

4.2 ミドルウェア
- 例外処理

4.3 ネットワーク
- 遠隔操作
- 機器間ネットワーク

4.4 組込みシステム
- メーター制御
- 航空機機器制御システム
- 船舶通信システム
- センサー入力処理

MCBOK2008: ソフトウェア開発のためのモデル検査知識体系
(算譜科学研究速報)
発行日：2009 年 8 月 3 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

MCBOK2008: Model Checking Body of Knowledge for software development
(in Japanese)
(Programming Science Technical Report)
Aug. 3, 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-J00022-99