

実務家のための形式手法

厳密な仕様記述を志すための形式手法入門 第二版

参考資料

独立行政法人 産業技術総合研究所事例



(独)産業技術総合研究所 組込みシステム技術連携研究体は、
自組織のシステム検証の科学技術に関する事例研究を集めて公開している。

項番	名称	題材の形態	手法	使用したツール
事例1	通信プロトコル設計へのモデル検査適用事例	仕様書	モデル検査	Uppaal
事例2	Webアプリケーションの基本設計書の検証	仕様書	モデル検査	Uppaal
事例3	Webアプリケーションの画面遷移仕様のモデル検査	仕様書	モデル検査	SMV, NuSMV
事例4	Webアプリケーションのクラス設計仕様に対するモデル化と検証	仕様書	モデル検査	Uppaal
事例5	自動検計システム仕様書のモデル検査	仕様書	モデル検査	SMV, NuSMV
事例6	遷移系抽象化アルゴリズムの検証	ソースコード	定理証明・対話型検証	PVS
事例7	モデル検査支援装置の基本デザインの検討	その他	その他	その他
事例8	アセンブラで記述された組込みシステムのモデル検査による検証事例	仕様書 ソースコード	モデル検査	Spin
事例9	一般公開で用いたLEGO用プログラムの検証	ソースコード	モデル検査	Uppaal
事例10	確率モデル検査による1次元イジングモデルの検証	その他	モデル検査	PRISM
事例11	便益性評価のためのデータ収集実験と評価	仕様書	その他	Uppaal
事例12	相互再帰的に定義された文字列を翻訳処理するプログラムの検証	ソースコード	定理証明・対話型検証	PVS
事例13	たし算かけ算プログラムのコンパイラの正当性証明	ソースコード	定理証明・対話型検証	Agda
事例14	非自動はかりの重量データ処理プログラムのモデル検査適用事例	仕様書	モデル検査	SMV, NuSMV
事例15	クルーズコントロールシステムの演繹的検証	仕様書	定理証明・対話型検証	Agda
事例16	Hoare論理の健全性のAgdaによる検証	その他	定理証明・対話型検証	Agda
事例17	Deutsch-Schörr-Waltemer-キングアルゴリズムのAgda-MLAT連携による検証	その他	定理証明・対話型検証	MLAT Agda
事例18	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	仕様書	定理証明・対話型検証	その他
事例19	リスト反転アルゴリズムのAgda-MLAT連携による検証	ソースコード	モデル検査 定理証明・対話型検証	MLAT Agda
事例20	TACC業務フロー図の検証	仕様書	その他	AIST workflow verifier
事例21	環境ドライバを用いた組込みシステムのソースコードモデル検査	仕様書 ソースコード	モデル検査	Spin
事例22	検証期間の調査のための車載組込みシステムに対するモデル検査実験	ソースコード	モデル検査	Spin
事例23	Java の例外処理のSPIN による検証	ソースコード	モデル検査	Spin Jex
事例24	ソフトウェア更新システムのモデル検査器を使った安全性の検証	仕様書 その他	モデル検査	Spin
事例25	Real-Time Maude によるモデル検査と検査式・モデルの修正	仕様書	モデル検査	Maude
事例26	制御系ECU調停器の演繹的検証	その他	定理証明・対話型検証	Agda
事例27	YAMPIIライブラリ中のポインタ操作のAgda-IVEによる検証	ソースコード	定理証明・対話型検証	MLAT Agda
事例28	システムLSI仕様の形式化と検証項目自動生成	仕様書	その他	Agda
事例29	仕様処理システムの適用実験事例	仕様書	その他	Agda

左の表は下記から作成
出典 検証事例報告集

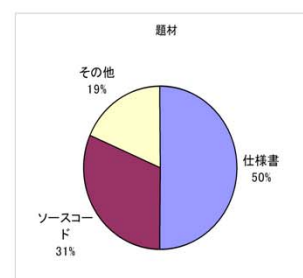
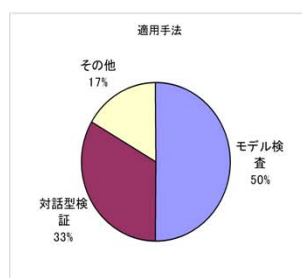
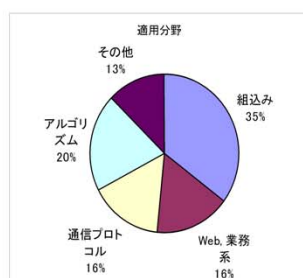
<http://cfv.jp/cvs/introduction/case.php>

独立行政法人 産業技術総合研究所事例



■ システム検証の事例報告集(2009年度版)

- 産業技術総合研究所 システム検証ラボ/システム検証研究センター/組込みシステム技術連携研究体が実施した事例(2002年度～)
 - 約1/3が組込み系への適用である
 - 殆どが形式検証, 特にモデル検査が約 50% を占める
 - 仕様書に形式手法を適用している事例が約50%を占める
 - 29事例中 19例を企業との共同研究として実施



出典:「2009年度版システム検証の事例報告集」産業技術総合研究所 組込みシステム技術連携研究体

独立行政法人 産業技術総合研究所事例



■ 主な事例の内容

項番	適用事例	達成目的	効果	分野・題材	手法
5	自動検針システム仕様の検証	仕様書の査読に代わる検証手段の確立	<ul style="list-style-type: none"> ・査読では見つからなかった仕様中の矛盾、記述不足の不具合をモデル検査で発見した。 ・2つの仕様の衝突の発見。同時には起こらないはずの2つの事象が同時に起こることを反例によって確認した。 ・仕様の記述不足。定常状態に戻らないという反例から、システムが「フリーズ」したときの対応が定義されていないことが判明した。 	組込みシステム・仕様書	モデル検査
22	モデル検査実施コストの調査	システム開発でモデル検査を実施する際の人的コスト測定	<ul style="list-style-type: none"> ・モデル検査のコストに関するデータを得た。 ・検査プロセスにかかる作業量の測定。検査対象の確認、モデル化、検査実施、モデル改良、検査完了まで10人日。 ・周期タスク駆動型組込みソフトウェアのモデル検査プロセスを提案した。 ・タスクのメインループ、関数呼び出しのモデル化、検査式のパターンなど作業手順の整理、モデル抽象化のノウハウ蓄積 	組込みシステム・ソースコード	モデル検査
29	電気ポット(*)の形式仕様記述	形式仕様作成ツールの評価	<ul style="list-style-type: none"> ・仕様の形式化プロセスを定め、専用ツールを用いて形式仕様を作成した。 ・仕様書の用語集作成。仕様の抽出をツール支援で実現。「統一仕様書式」で表現された仕様を保持した。 ・「統一仕様書式」で書かれた仕様を形式仕様へ自動変換。型検査で整合性を確認した。 	組込みシステム・仕様書	形式仕様記述

(*)「話題沸騰ポット要求仕様書(GOMA-1015型)第七版」組込みソフトウェア管理者・技術者育成研究会(SESSAME)作成
出典:「2009年度版システム検証の事例報告集」産業技術総合研究所 組込みシステム技術連携研究体

形式手法の適用事例



項番	適用事例	適用範囲	開発成果、他
1	コピー複合機内の制御ソフトウェア	モデル検査 (SPIN)	検証対象のインタフェースマネージャはクラス数が60-80個。 自動コード生成後のソースコード行数は約6万行。 検証した状態数は1万個程度。 適用の実際の効果に関して、テストで再現性の無い取りづらいバグの全てを取ることはできないものの、詳細設計段階において、高ストレス下で発生する可能性のある不具合を発見することができた(ストレステストの前倒し)。
2	携帯電話ICチップファームウェア	設計工程での仕様記述(VDM)	形式仕様の記述量はテストケースも含めて10万行程度。 実装コードは11万行程度。 フェリカ社で開発したモバイル FeliCa IC チップファームウェアは、Common Criteria(CC) の EAL4+ALC.FLR.1+AVA.VLA.3 の認証取得。
3	ICカードのCC認証 EAL4+(ADV.SPM.3)	・要求、アーキテクチャ、仕様、コードの対応付け ・電子パスポートアプリケーションのセキュリティ要求を	セキュリティ要求の検証手順、追跡性の確認、形式手法の適用範囲等の検討。

IPA/SEC「高信頼性システム開発技術の動向～形式手法を中心として～」から作成

形式手法の適用事例



項番	適用事例	適用範囲	開発成果、他
4	防潮可動堤開閉意思決定システム／オランダ	SPINを用いたモデリングおよび検証 (SPIN) プロセス・アーキテクチャおよび外部システムとの通信についてモデリングと検証 データとアルゴリズム解析 (Zを使用) 機能および各プロセスにおけるデータのストアとフローについてモデリング	<ul style="list-style-type: none"> ■ソフトウェアに重大な欠陥は発見されず、ソフトウェア品質に問題がないことが確認された。 ■Zを用いたモデリングを経験：テスト実施者やレビュー実施者はテスト・ケース作成やコード・設計のレビューを効率的に行えるようになった。 ■各工程間のコミュニケーション促進・曖昧さの解消に役立った。(設計者、プログラマ、テスト実施者・コードレビュー実施者、保守作業における人的要素を過小評価をしないこと) ■ソフトウェア設計は元より、HWやパーツの寿命を勘案した保守活動全般が重要であり、留意すべきことがわかった。 ■仕様記述・モデルテスト・コードレビューが連携した。 ■IEC 61508、SIL4相当に対応できた。
5	航空管制システム：IFACT／イギリス	機能仕様記述 (Z) コーディング (SPARKが90%) テスト、検証	不具合の大幅な削減(具体的な数値は公表していない)信頼性の高いシステムの実現(具体的な数値は公表していない) 生産性についての公表はしていないが、一般的なこととして、形式手法の採用により、信頼性は向上するが、生産性の向上は見込まれない(同等、もしくは悪くなる)。
6	無人地下鉄車両の制御 (バリエ地下鉄14号線)	仕様記述 自動コード生成 検証 妥当性検討	1998年に自動運転を開始した無人運転システムであり、車載制御システムを搭載する列車と、搭載しないシステムを同時運行できる。Bメソッドが利用された初めてのアプリケーションとして成功した。すべての不具合は開発プロセスで発見され、妥当性検証は単体テストをすることなく、効率的に実施できた。 システムの安全系はB手法を用いて確認された。証明(Proof)の後、機能検証、統合検証、オンサイトテスト、運用においてバグは発見されていない。 Bメソッドを利用した初めてのプロジェクトであったため、STS(IBMATRA)の技術者35名、RATPの技術者15名という多数の技術者とシステム全体で4年の開発年月を要した。ここでの成果が以降の類似プロジェクトの基盤となった。
7	バリエ地下鉄プラットフォームドアの制御	<ul style="list-style-type: none"> ■機能分析での形式手法適用 SOW(statement of work)の完全性と曖昧自由度を評価 他 ■システム開発における形式手法適用 システム仕様とソフトウェア仕様 モデルのチェック、適切性の内部検証 他 	プラットフォーム上のドア制御システムにおいてもBが用いられているが、この事例を通して、Bの使用法や、鉄道産業における成功度を明らかにすることを目指している。

IPA/SEC「形式手法適用調査報告書」(2010年7月29日公開)から作成

SEC-FM1-08-2

Copyright © 2012,2013 IPA

IPA Software Engineering Center

6

形式手法の適用事例



項番	適用事例	適用範囲	開発成果、他
8	シャルルドゴール空港の無人シャトル制御	B手法でモデル記述、詳細化、検証を行い、ADAコードを自動生成。安全系ソフトウェアの部分はBで設計され、Ada(Digisafe Ada)に変換。	開発されたソフトウェアはIEC 61508 : EN 50126, EN 50128, EN 50129に準拠し、SIL4に分類された。 ADAに変換されたツールは、従来プロセスで手動で開発されたコードより10%程度速くなった。これは詳細化(リファインメントルール)によるものであり、最終的に詳細化のルールを修正することで対応した。 構築されたBモデルは、約183,987行、このうち抽象モデルが28,163で全体の約15%(マニュアルで作成)であり、詳細化により自動で作成された具体モデルが、約128,000行(70%)であった。 全体で43,000程度の証明課題が存在し、このうち1,400程度(3%)がマニュアルでインタラクティブに証明され、その他は、AtelierBIにより自動証明することができた。ADAの実行コード数は、158,612行となった。
9	北京地下鉄の自動列車停止システム	仕様設計、実装	仕様設計で発注元のチームがすべての機能を形式化した。この仕様を元に受注先の技術者が発注元のチームと連携して、Bメソッドを適用し、仕様を形式化し、微調整した後、最終的にAdaに変換した。
10	Sao Paulo地下鉄プラットフォームドア	機能仕様 モデル作成 コード生成 検証	短期間(3ヶ月)に、仕様の開発、モデル開発、コードの自動生成(約10,000行)を実現した。 現在(2009年10月)、クライアントによるバリデーションを実施中。 プロジェクトの開発期限は非常に短く、SIL3認定のために、ソフトウェアのソースコード開発を含むV&Vの開発プロセスを必要とした。 SCADEは、Cコード生成でSIL3, 4の認定を支援する唯一のツールであった。 SCADEのモデリング機能により、仕様からコーディングまでの機能的アプローチを提供することで、短期の開発期間に間に合うことができた。 *当初は、Bメソッドの利用を検討したが、形式手法やツールの習得に時間がかかることが予測されたため、比較的導入が容易であるSCADEを採用することとなった。
11	ニューヨーク地下鉄カーネル線列車制御システム(CBTC)の最新化	CBTCの開発にBメソッドが使われている	詳細化ツールの導入により、パリ地下鉄14号線と比較し大幅に開発効率が向上した。パリ14号線の開発規模に比べ、B表記の行数で約2.5倍になっているにも係らず、開発期間は約1年と短く、投入人数も4名となっている。
12	Airbus社製航空機のシステム	モデル開発 シミュレーション 検証 自動コード生成	1. コーディングエラーの大幅な削減: Airbus A340 プロジェクトでは70%のコードが自動生成された。 2. 仕様変更への迅速な対応: システムモデルの仕様変更迅速に対応可能(仕様変更のターンアラウンドサイクルが3~4倍改善)にし、トレーサビリティも改善された。 3. 生産性の改善: 生産性が改善したことでソフトウェア規模の増大に対応することができた。 A340のプロジェクトでは、SCADEを利用することで、大幅な効率化を実現したため、SCADEをA380の開発にも採用した。 A380では、Airbus社とサプライヤがSCADEを使用した。

IPA/SEC「形式手法適用調査報告書」(2010年7月29日公開)から作成

形式手法の適用事例



項番	適用事例	適用範囲	開発成果、他
13	艦載ヘリコプタ運行 限界計装システム (SHOLIS)	仕様記述: Z 証明(Proof) ソフトウェア記述: SPARK	Integrity: SIL4 ソフトウェア規模: 27000行(SPARK) Defect/ksLOC: 0.22 LOC/Day: 7 Proofによる実証は、テストを実施するより、コスト面で有利であった。
14	コンポーネント仕様 のモデル化(ブジョー)	部品の機能仕様の形式化 ・Bモデル化 ・ディクショナリ ・記録分析	206、307、407モデルのモデル化 200万行の設計書に記述された52の機能についてモデル化を行った。2車種で実施(307、206)ー約 2 x 150,000行の書類が作成された。ー50のBモデル、7000のイベント、2000の抽象変数で記述された。これにより98%の証明が自動的に実行された。BI の理論は、PSAが保有している。ブジョーの技術者が診断テストを定義し、PSAのホットラインの技術者が利用している。
15	「Tokeneer ID Station (TIS)」 (バイオメトリクスID認証 ツールのアクセス管理セ キュリティソフトウェア) (NSA)	要求仕様分析 セキュリティ分析 仕様作成 設計 実装 システムテスト	個別の信頼性テストと2003年の納入以来、発見された欠陥は4個であった。 その1つは、プロジェクト完了後のコードテストで発見された。2つめのバグは、証明(Proof)を実施中に発見された。ファイルから読み込まれた整数を検証するコードのバグで、「秒(Seconds)」を表わす整数が、1/10秒に変換される際にオーバーフローエラーを起こした。SPARKツールは、部分的コレクティネスとランタイムエラーの検証条件を生成するが、Adaのオーバーフローチェックの検証条件が生成されなかった。その後のツールの改善で検証条件が再生成されバグが発見された。その他にSPRE社のプロジェクトチームがテストで障害を発見した。両社とも、TISのコアの間違いよりも、ユーザマニュアルの不備を心配している。納入以来、システム分析のための利用や試行では欠陥は発見されなかった。工数比率のシステムテストには、SPRE社のテストへの貢献は入っていない。おそらく25%ほどと推測される。機能仕様は、100ページほどのZ表記と英文の説明から構成される。NSAからの依頼は、EAL5に準拠するシステムの開発であった。Praxisは、多くの領域でEAL5の要求以上の条件を達成した。厳格な技術を使用したことが結果的に効率的であったと言う。

IPA/SEC「形式手法適用調査報告書」(2010年7月29日公開)から作成

参考資料



【日本語の教科書】

- 荒木 啓二郎, 張 漢明: プログラム仕様記述論, オーム社, 2002年11月
<http://dontaku.csce.kyushu-u.ac.jp/books/ProgramSpecification/>
[形式手法の基本に重点を置いた、入門用教科書](#)
- 荒木 啓二郎, 張 漢明, 荻野 隆彦, 佐原 伸, 染谷 誠(共訳): ソフトウェア開発のモデル化技法, 岩波書店, 2003年2月
[John Fitzgerald and Peter Larsen: Modelling Systems : Practical Tools and Techniques in Software Development, Cambridge University Press, 1998]
- 酒匂 寛(訳): VDM++ によるオブジェクト指向システムの高品質設計と検証, 翔泳社, 2010年8月
[John Fitzgerald, Peter Larsen, Peter Gorm Larsen, Paul Mukherjee, and Nico Plat: Modelling Systems : Validated Designs for Object-oriented Systems, Springer-Verlag, 2004]
[理論面より実際のモデル構築に重点を置いたVDM++の入門用教科書](#)
- 荒木啓二郎(監修), 石川冬樹: VDM++ による形式仕様記述, 近代科学社, 2011年7月

SEC-FM1-08-2

Copyright © 2012,2013 IPA

IPA Software Engineering Center

9

[プログラム仕様記述論]

VDMの例も出てくるが、形式手法の初歩の初歩の話を書いていて、上記の本のスタートとなる話が展開されている。

VDMの例やZの例題つき。

[VDM++ によるオブジェクト指向システムの高品質設計と検証]

原書著者のジョン・フィッツジェラルドはVDMの証明の先生、ピーター・ゴラム・ラーセンはovertureを作った。

ポール・マッカージーとニコ・プラットはラーセンと一緒にコンサルティング、モデル化などを行っている技術者。

ニコ・プラットはVDMのISO標準に関わった。

マーセル・バーホフはオランダで市場(いちば)のモデルを作った人で開発現場にしながら、研究開発部門にいて、EUの研究プロジェクトのリーダーである。

翻訳としては、酒匂さんは優秀なエンジニアで、英語にも堪能なのできちんとしたものとなっている。

参考資料



- 酒匂 寛(訳):オブジェクト指向入門 第2版 原則・コンセプト, 翔泳社, 2007年1月
[Bertrand Meyer: Object-Oriented Software Construction, Prentice Hall, 2000]
- 来間啓伸 : Bメソッドによる形式仕様記述, 近代科学社, 2007年
- 中島震: SPINモデル検査, 近代科学社, 2008年
- 萩谷昌己(監修), 吉岡 信和, 青木 利晃, 田原 康之: SPINによる設計モデル検証, 近代科学社, 2008年
- 佐原 伸: ～ソフトウェアトラブルを予防する～形式手法の技術講座, ソフト・リサーチ・センター, 2008年
[開発現場で実際のモデル構築を行うノウハウを記述した入門用教科書](#)
- 産業技術総合研究所システム検証研究センター: モデル検査[初級編]—基礎から実践まで4日で学べる—, ナノオプトメディア, 近代科学社, 2009年11月
- 産業技術総合研究所システム検証研究センター: モデル検査[上級編] —実践のための三つの技法, ナノオプトメディア, 近代科学社, 2010年2月
- Mordechai Ben-Ari, 中島 震(監訳), 谷津 弘一, 野中 哲, 足立 太郎(共訳): SPINモデル検査入門, オーム社, 2010年3月

SEC-FM1-08-2

Copyright © 2012,2013 IPA

IPA Software Engineering Center

10

[オブジェクト指向入門 第2版]

こちらには原則とコンセプトと書かれているが、はもうひとつあって、それと合わせると1800ページほどになるが、それらを読むと、構造化やオブジェクト指向契約による設計だとかの歴史がほとんど理解できるものとなっている。

[形式手法の技術講座]

他の本に書かれていないような、仕様を書く上でのアーキテクチャの話について書かれている。

参考資料



【普及や人材育成に関して有用な論文】

- J. A. Hall: Seven Myths of Formal Methods, IEEE Software, Vol.7, No.5, pp.11–19, 1990
- J. P. Bowen and M. G. Hinchey: Seven More Myths of Formal Methods, IEEE Software, Vol.12, No.4, pp.34–41, 1995
- J. P. Bowen and M. G. Hinchey: Ten Commandments of Formal Methods, IEEE Computer, Vol.28, No.4, pp.56–63, 1995
- J. P. Bowen and M. G. Hinchey: Ten Commandments of Formal Methods...Ten Years Later, IEEE Computer, Vol.39, No.1, pp.40–48, 2006
- Keijiro Araki: Are Formal Methods Relevant? – How to Explode the Seven Myths in Japan–, Proc. APSEC’95, pp.514–515, 1995
- Keijiro Araki and Han-Myung Chang: Formal Methods in Japan–Current State, Problems, and Challenges–, Proc.VDM 2002,Third VDM Workshop, 2002
- Jean-Raymond Abrial: Formal Methods in Industry: Achievements, Problems, Future, Proceedings of ICSE2006, 2006

参考資料



- Robert M. Hierons, Kirill Bogdanov, Jonathan P. Bowen, Rance Cleaveland, John Derrick, Jeremy Dick, Marian Gheorghe, Mark Harman, Kalpesh Kapoor, Paul Krause, Gerald Luttgen, Anthony J. H. Simons, Sergiy Vilkomir, Martin R. Woodward, Hussein Zedan: Using Formal Specifications to Support Testing, ACM Computing Surveys, Vol.41, No.2, February 2009
- Special Issue on Software Verification, ACM Computing Surveys, Vol.41, No.4, October 2009
 - Jim Woodcock, Peter Gorm Larsen, Juan Bicarregui, and John Fitzgerald: Formal Methods, Practice and Experience, article no. 19, pp.1-36
- Steven P. Miller, Michael W. Whalen, and Darren D. Cofer: Software Model Checking Takes Off, Communications of ACM, Vol.53, No.2, pp.58-64, February 2010
- Ciera Jaspan, Michael Keeling, Larry Maccherone, Gabriel L. Zenarosa, Mary Shaw: Software Mythbusters Explore Formal Methods, IEEE Software, vol.26, no.6, pp.60-63, Nov/Dec 2009
- Barry W. Boehm: Software Engineering Economics, Prentice Hall, 1981

[Software Engineering Economics]

統計データに基づく、ソフトウェア・プロジェクト分析・見積のバイブル

見積手法COCOMOの教科書でもある

参考資料



【日本語の記事/論文】(ごく一部)

- 進藤: 特集ソフトウェアは硬い, 日経エレクトロニクス, No.915, 2005年12月19日号
- 中島 震: 形式手法の実像を知る, 日経エレクトロニクス, No.933, 2006年 8月28日号
- 栗田 太郎: 仕様書の記述力を鍛える—モバイルFeliCa開発における形式仕様記述の導入事例, 日経エレクトロニクス, 2007年 2月12日号, PP.133-152, 2007年2月
- 佐原 伸, 荒木 啓二郎: オブジェクト指向形式仕様記述言語VDM++支援ツールVDMTools, コンピュータソフトウェ, Vol.24, No.2, pp.14-20, 2007年4月
- 荒木 啓二郎: フォーマルメソッドの過去・現在・未来=適用の実践に向けて, 情報処理Vol.49, No.5, PP.493-498, 2008年5月
- 栗田太郎: 携帯電話組み込み用モバイル FeliCa IC チップ開発における形式仕様記述手法の適用, 情報処理情報処理Vol.49, No.5, pp.506-513, 2008年5月
- 栗田 太郎, 荒木 啓二郎: モデル規範型形式手法VDMと仕様記述言語VDM++—高信頼性システムの開発に向けて—, 日本信頼性学会誌「信頼性」, Vol.31, No.6, pp.394-403, 2009年9月

参考資料



- 藤枝 純教: 経営者はアーキテクチャと形式手法を忘れてはいけない, SEC journal, No.20, 2010年3月
- 荒木 啓二郎: ソフトウェア開発現場への形式手法導入— 形式手法適用の実験から得られた知見—, SEC journal, No.21, 2010年6月
- 栗田太郎: 形式手法の実践に対してよく尋ねられる質問とその回答 — モバイル FeliCa の開発における形式手法記述を通して, SEC journal, No.24, 2011年3月
- 株式会社 三菱総合研究所: フォーマルメソッド導入ガイダンス, 2011年6月
<http://formal.mri.co.jp/method/>
- 荒木啓二郎: 形式手法導入のための産学連携 PBL の活用, SEC journal, No.27, 2012年1月
- 独立行政法人情報処理推進機構 形式手法活用ガイド
<http://sec.ipa.go.jp/reports/20120928.html>

参考資料



【調査報告書】

- 独立行政法人産業技術総合研究所 組込みシステム技術連携研究体,
 - 検証事例報告集
<http://cfv.jp/cvs/introduction/case.php>
- 独立行政法人情報処理推進機構:
 - 高信頼ソフトウェア構築技術に関する動向調査 調査報告書 (2008年6月6日公開)
<http://sec.ipa.go.jp/reports/20080606.html>
 - 高信頼性システム開発技術の動向～形式手法を中心として～ (2010年3月3日公開)
第3章「形式手法の適用事例」
<http://sec.ipa.go.jp/reports/20100331c.html>
 - 形式手法適用調査 調査報告書 (2010年7月29日公開)
<http://sec.ipa.go.jp/reports/20100729.html>
 - 情報系の実稼働システムを対象とした形式手法適用実験報告書 (2012年4月20日公開)
<http://sec.ipa.go.jp/reports/20120420.html>
- Dependable Software Forum (DSF)
 - 「JEITAソフトウェアエンジニアリング技術分科会ワークショップ2010資料」
<http://www.nttdata.com/jp/ja/dsf/data.html>

参考資料



【SEC journal 掲載記事】

- ソフトウェア開発における形式手法の適用と普及の方策を考える (No.11)
- 形式検証による組込みソフトウェア検証の実用化 SEC 2007年度活動概要 共同研究 (No.14)
- 高信頼ソフトウェア領域 SEC 2007年度活動概要 エンタプライズ系 (No.14)
- 経営者はアーキテクチャと形式手法を忘れてはいけない (No.20)
- ソフトウェア開発現場への形式手法導入 -形式手法適用の実経験から得られた知見- (No.21)
- 独立検証及び妥当性確認と形式手法がもたらすソフトウェア開発プロセスの高信頼化 (No.22)
- 形式手法の実践に対してよく尋ねられる質問とその回答
モバイルFeliCaの開発における形式仕様記述を通して (No.24)
- 構造化日本語仕様書としてのVDM仕様 (No.24)
- 地方独立行政法人 北海道立総合研究機構 工業試験場
-新組織と組込みシステム開発技術による道内企業への技術支援の取り組み- (No.25)
- ソフトウェアの高信頼化手法の実践にむけて SEC 2010年度活動概要 統合系 (No.25)
- 形式手法導入のための産学連携PBLの活用 (No.27)
- 形式手法・モデルベース開発技術の推進 SEC 2011年度活動概要 統合系 (No.29)
- 形式手法入門教材の開発 形式手法はハードルが高いという誤解を払拭するために (No.30)

参考資料



【VDM言語仕様】

- SCSK Corporation. VDM-SL 言語マニュアル. SCSK Corporation, 第 1.2 版, 2012. Revised for VDMTools V9.0.2.
- SCSK Corporation. VDM++ 言語マニュアル. SCSK Corporation, 第 1.2 版, 2012. Revised for VDMTools V9.0.2.
- 佐原伸. 形式手法の技術講座—ソフトウェアトラブルを予防する. ソフトリサーチセンター, 2008.



実務家のための形式手法

厳密な仕様記述を志すための形式手法入門

参考資料

独立行政法人情報処理推進機構
技術本部 ソフトウェア・エンジニアリング・センター
統合系システム・ソフトウェア信頼性基盤整備推進委員会
上流品質技術部会 人材育成WG(編)
2013年3月 第二版発行

記載されている個々の情報に関しての著作権及び商標はそれぞれの権利者に帰属するものです
なお、本書の内容は将来予告なしに変更することがあります