

# フォーマルアプローチ小特集 論文募集

フォーマルアプローチ（形式手法・形式技法・形式理論）は、情報システムや組込みシステムの設計開発における信頼性向上の鍵となる重要な基盤です。これまで、設計対象のモデル化、要求分析と仕様記述、コード自動生成、テストと検証、保守と再利用などに関する技術と理論的知見を生み出してきました。近年の情報技術の進展に伴う対象領域の拡大に伴い、フォーマルアプローチは従来にも増して多様な分野で用いられるようになり、ますます発展しています。

本小特集は、情報システムや組込みシステムの設計・運用におけるフォーマルアプローチについて、基礎理論から応用まで、幅広い研究を対象にしています。個別の対象領域に特化したケーススタディから、分野横断的な手法や理論まで、様々な方面から、フォーマルアプローチ研究に携わる若手研究者を奨励するとともに、この分野の研究が更に発展することを目指しております。

奮って御投稿下さいますよう御案内申し上げます。

## 1. 対象分野

主な対象は以下の通りですが、これに限らず、

情報システムや組込みシステムおよびそれをとりまく環境を定式化した上で、そのシステムの振舞いの解析や性質の導出を厳密に行い、設計・運用に関わる種々の問題の解決を図る

ことを目指した論文を広く募集します。

- **基礎理論:**  
システムの構造や振舞いの形式記述・検証に関する基礎理論
- **形式技法:**  
ソフトウェアやハードウェアを形式的に記述・検証するための技法
- **形式ツール:**  
モデル検査器や定理証明器など、形式手法に基づくツール
- **応用:**  
情報システムや組込システムへの形式手法の適用事例

## 2. 論文の執筆と取扱い

論文（一般論文）、レター、及びサーベイ論文を募集します。投稿規定等は電子情報通信学会の英文誌の規定と同じです。以下の規定を御参照ください。

“The Information for Authors”  
(IEICE Transactions on Information and Systems)  
[http://www.ieice.org/eng/shiori/mokuji\\_iss.html](http://www.ieice.org/eng/shiori/mokuji_iss.html)

## 3. 投稿方法

本小特集では、電子投稿のみを受付けます。

ステップ1. 論文を下記のweb pageから投稿して下さい。初期投稿時に、編集可能な論文本体(TeX/Word)、図、著者の写真、biographyも投稿する必要があります。

[https://review.ieice.org/regist\\_e.aspx](https://review.ieice.org/regist_e.aspx)

投稿の際には以下の項目を選択して下さい。

“Journal/Section” → “[Special FO] Formal Approach”

データ登録時点で論文原稿のアップロードができない場合、「郵送による投稿」を選択して登録を一旦完了させて下さい。論文原稿のアップロードは、登録後に送付される電子メールに記載のURL にアクセスして行って下さい。

ステップ2. 仮登録後に作成される“Copyright Transfer and Page Charge Agreement”と“Confirmation Sheet of Manuscript Registration”に記入、署名し、論文投稿締切日までに下記問合せ先まで電子メールまたは郵便にてお送り下さい(電子メールが望ましいです)。郵送の場合、封筒に『フォーマルアプローチ小特集』と記載して下さい。

## 4. 主なスケジュール

- |             |                         |
|-------------|-------------------------|
| ● 論文投稿締切    | 平成25年7月17日(水) 23:59 JST |
| ● 第一回判定通知予定 | 平成25年9月12日              |
| ● 最終判定予定    | 平成25年12月20日             |
| ● 発行予定      | 平成26年5月号                |

## 5. 小特集 編集委員会

委員長 磯部 祥尚(産総研)  
幹事 岡野 浩三(阪大), 河辺 義信(愛知工大), 土屋 達弘(阪大)  
委員 青木 利晃(北陸先端大), 石川 冬樹(情報研), 來間啓伸(日立),  
小林 孝一(北陸先端大), 寺内 多智弘(名大),  
中村 正樹(富山県立大), 蓮尾 一郎(東大)

## 6. 問合せ先

磯部 祥尚  
fa-submit-ml(at)aist.go.jp  
〒305-8568 茨城県つくば市梅園1-1-1 中央第2  
産業技術総合研究所セキュアシステム研究部門

本特集のホームページ:

和文 <http://staff.aist.go.jp/y-isobe/FA/index-j.html>

## 7. 注意事項

- 論文が採録となった場合、掲載料(論文別刷代金を含む)をお支払い頂くことになります。
- 投稿に際し、著者のうち少なくとも1名は、本会会員でなければなりません。投稿資格を満たさない著者からのご投稿は受け付けません。入会の案内は  
<http://www.ieice.org/jpn/nyukai/index.html>  
をご覧ください。

---

# フォーマルアプローチ特集 過去の掲載論文

## 第1回掲載論文（2006年4月号）

### [計算モデル]

ステータス付き再帰的経路順序による項書換え系多重完備化手続き  
 $\pi$  計算に対する時間拡張と合同的性質  
時相論理の充足可能性判定器のための性能評価法

### [ハードウェア]

状態遷移表現への変換に基づくハードウェア/ソフトウェア協調設計の形式的検証手法  
高位仕様記述からの非同期回路自動合成について  
データベース形式検証のための入力制約を考慮したモニタ回路生成手法

### [ソフトウェア]

時間制約を保証するUML/OCLを用いた分散実時間アプリケーション開発手法  
モデル生成法に基づくJavaScriptプログラム型検査の機械実行  
XML文書に対するアクセシビリティ・ガイドライン適合性検証

### [セキュリティ]

第三者機関を利用したワンタイムIDシステムの設計, および様相論理による安全性検証  
UMLによるプロテクションプロファイルのモデル化とその形式的検証

## 第2回掲載論文（2007年4月号）

### [基礎理論]

単純型項書換え系上の依存対法における実効規則と直積型項へのラベル付け  
XMLデータベースにおけるスキーマ進化のための更新操作群とそれらのスキーマ表現能力保存に関する性質

### [ソフトウェア]

制約指向に基づいたUMLモデルの不整合検出・解消手法の提案

## 第3回掲載論文（2008年4月号）

### [セキュリティ]

実行履歴に基づくアクセス制御の形式モデルと検証  
Task-Structured PIOAフレームワークを用いた適応的攻撃者に対するDiffie-Hellman鍵交換の安全性解析

### [データベース]

書き換えに基づく最適化のためのXQueryの相対コストモデル

## 第4回掲載論文・和文（2009年5月号）

### [モデル検査]

【招待論文】時間オートマトンのモデル検査

### [セキュリティ]

【招待論文】汎用的結合可能性による暗号システムの安全性証明  
記号論的暗号解析を用いた Oblivious Transfer プロトコルの解析

## 第4回掲載論文・英文（2009年5月号）

### [Hardware verification]

Word-level equivalence checking in bit-level accuracy with identical datapath  
A unified framework for equivalence verification of datapath oriented applications

### [Foundation]

Pre- and post-conditions expressed in variants of the modal  $\mu$ -calculus

### [Model checking]

Probabilistic model checking of the one-dimensional ising model

### [Software testing]

Generating test cases from proof scores in the OTS/CafeOBJ method

### [Security]

Comparison of the expressive power of language-based access control models  
Verification of the security against inference attacks on XML databases

## 第5回掲載論文（2010年5月号）

### [Term rewriting systems]

Multi-context rewriting induction with termination checkers  
Decidability of termination and innermost termination for term rewriting systems with right-shallow dependency pairs

### [Program transformation]

Program transformation templates for tupling based on term rewriting

### [Formal Specification]

Towards reliable e-government systems with the OTS/CafeOBJ method

### [Program Analysis]

Over-approximated control flow graph construction on pure Esterel

### [Model Checking]

An abstraction refinement technique for timed automata based on counterexample-guided abstraction refinement loop

### [Software Testing]

Computer algebra system as test generation system

---

---

# フォーマルアプローチ特集 過去の掲載論文

## 第6回掲載論文（2011年5月号）

### [Model Checking]

An SMT-based Approach to Bounded Model Checking of Designs in State Transition Matrix  
Probabilistic Symmetry Reduction for a System with Ring Buffer

### [System Analysis]

QoS Analysis of Real-time Distributed Systems Based on Hybrid Analysis of Probabilistic Model Checking Techniques and Simulation

### [Specification Translation]

Translation of State Machines from Equational Theories into Rewrite Theories with Tool Support

### [Software Development Methodology]

Modeling, Verification and Testing of Web Applications Using Model Checker

## 第7回掲載論文（2012年5月号）

### [Formal Methods]

Formal Verification of Effectiveness of Control Activities in Business Processes  
Refactoring Problem of Acyclic Extended Free Choice Workflow Nets to Acyclic Well-Structured Workflow Nets

### [Model Checking]

Efficient Multi-Valued Bounded Model Checking for LTL over Quasi-Boolean Algebras

### [Database Security]

Decidability of the Security against Inference Attacks using a Functional Dependency on XML Databases

### [System Analysis]

Stochastic Power Minimization of Real-Time Tasks with Probabilistic Computations under Discrete Clock Frequencies

## 第8回掲載論文（2013年6月号）

---