会議レポート

ETAPS 2006 参加報告

2006 年 3 月 25 日から 4 月 2 日まで，ETAPS 2006（The European Joint Conferences on Theory and Practice of Software）に参加した．ETAPS はソフトウェア科学に関するヨーロッパの主要国際会議で，今回が第 9 回目である．オーストリアのウィーン市内中心部にあるウィーン工科大の電気工学科棟に，666 名（日本から 15 名）の参加者が集った．

ETAPS は単独の会議ではなく，5 つのメイン会議

CC：International Conference on Compiler Construction

ESOP：European Symposium on Programming

FASE：Fundamental Approaches to Software Engineering

FOSSACS：Foundations of Software Science and Computation Structures

TACAS：Tools and Algorithms for the Construction and Analysis of Systems

を中心とし，さらに 18 のワークショップなどからなる[☆1]．ワークショップには，CMCS（coalgebra 理論），SPIN（システム検証ツール），WRLA（書き換え論理）など，興味深い会議が名を連ねた．セキュリティプロトコルの形式的検証に興味を持つ筆者は，WITS（Workshop on Issues in the Theory of Security）というワークショップで発表し，検証ツールに関する動向を知るべく TACAS を主に聴講した．

☆1 各会議の会議名・主催者・プログラムなどは，http://www.complang.tuwien.ac.at/etaps06/ を参照されたい．

TACAS での講演風景．

WITS での休憩時間．異なる会議への参加者同士も，盛んに交流していた．

WITS は，IFIP WG 1.7 主催のセキュリティ検証に関するワークショップで，第 6 回目を迎える．今年は招待講演 4 件と一般講演 15 件の発表があった．筆者は，電子投票プロトコルに対する匿名性の定理証明について発表した（“Backward simulations for anonymity”（Y. Kawabe et al.））．招待講演では，“Limits of the soundness of Dolev-Yao models”（B. Pfitzmann）が印象に残った．Dolev-Yao モデルはしばしばプロトコル検証に用いられているが，講演ではこのモデルがうまく扱えない場合（2 つの暗号メッセージ間に有意な長さの違いがある場合など）が紹介され，モデルに対する拡張の指針が示された．一般講演では，“Breaking and fixing public-key Kerberos”（I. Cervesato et al.）が印象に残った．講演者らは PKINIT プロトコルに対する新たな攻撃を見つけ，さらに改良版プロトコルがこの攻撃に耐えることを形式的に検証していた．PKINIT は Microsoft の Windows にも使われており，Cervesato らの指摘に基づき修正されたという．実システムの検証は，今後ますます重要になると感じた．

TACAS では，システム検証ツールの技法や実装について，数多くの発表があった．たとえば，

- “Towards combining SMT and interactive proof assistants”（P. Fontaine et al.）：定理証明系と SAT solver との融合
- “Verifying concurrent message-passing C programs with recursive calls”（S. Chaki et al.）：通信プログラムの形式化とモデル検査
- “MCMAS：a model checker for multi-agent systems”（A. Lomuscio et al.）：さまざまな知識論理のオペレータを扱えるモデル検査器

などである．これらの発表から，大規模システムに対する自動検証技術が進んでいることを実感した．

今回，会場となった建物ではいくつかの会議が常に開かれており，どの会議でも活発な議論が交わされていた．また，会場では「DAILY ETAPS」という新聞が毎日発行され，主催者や論文賞受賞者のインタビューが速報されていたのも面白かったと思う．次回の ETAPS は，2007 年 3 月 24 日から，ポルトガルのブラガ（Braga）で開かれる予定である．

（河辺義信／ NTT コミュニケーション科学基礎研究所）