要 旨

実行履歴に基づくアクセス制御に対するモデル検査の充足可能性判定器を用いた高速化

山本 風歌

システムの機密性を確保することを目的として，様々なアクセス制御技術が存在している．これらの中には，プログラミング言語の機能として提供されているものや実装が検討されているものもある．本研究では，Java で採用されているスタックベースアクセス制御（Stack-Based Access Control, SBAC）の脆弱性を修正した履歴ベースアクセス制御（History-Based Access Control, HBAC）の検証問題に着目する．

先行研究では，HBAC を利用したプログラムを形式的に表現し，文脈自由言語に基づいた検証を行う手法が示されている．しかし，この手法ではサイズの大きなモデルに対して検証が行えないか，検証に多大な時間がかかることがある．

そこで，本研究では HBAC を用いたプログラムの検証を，有界モデル検査の手法を応用して高速化する方法を提案する．有界モデル検査は，状態空間内の到達可能性を充足可能性問題に帰着して検査する手法であり，高速な充足可能性判定器の能力を活用して検証問題を解こうとするものである．本研究では，HBAC を用いたプログラムの検証を充足可能性問題に帰着する方法を提案する．また，提案手法を実装し，従来手法と比較して検証速度に改善が見られたか確認する．実際に提案手法を実装し，比較実験を行った結果，サイズの大きなモデルに対して，検証速度に優位性が見られた．

キーワード　モデル検査，充足可能性判定，アクセス制御

Abstract

A Fast Model-Checking Method of History-Based Access Control Programs Using a SAT-Solver

Fuka YAMAMOTO

There are many access control technologies for the purpose of ensuring the confidentiality of a system. Some of them are built in a programming language and is called language-based access control. History-based access control is one of the language-based access control technologies.

Previous studies have proposed a method for verifying the program using the history-based access control, based on the emptiness problem of context-free languages. However, this approach sometimes takes much time or cannot validate large models.

In this thesis, we propose a fast model-checking method of history-based access control programs based on the bounded model checking. The bounded model checking is a method for solving the verification problem by reducing it to the satisfiability problem. In many cases it can perform the search of the state space faster than conventional model-checking methods. We propose a method to convert the verification of history-based access control programs to the satisfiability problem. By performing experiments, it is confirmed that the proposed method can verify large programs faster than the method proposed by Takata et al.

key words model checking, satisfiability, access control