FW サーバシステムの検証に関する研究

横川　智良 (0510109)

北陸先端科学技術大学院大学 情報科学研究科

2008 年 2 月 6 日

キーワード: 検証, 定理証明, オブジェクト指向, モデリング.

概要

本稿では、検証対象である FW サーバシステムのオーディット・マネージャに対して、オブジェクト指向を用いたモデリング、定理証明器を用いた検証を行いその動作の正当性を証明した。

背景

今日、インターネットなど急速な情報インフラ網の発展により高度な情報化社会が構成されていく一方で、情報が財産となる現代、その流出が深刻な問題にとなっている。こうしたなかで従来に比べ、より信頼性の高い情報セキュリティ技術への関心が高まってきている。では、データのセキュリティを保つためには、どういった手段があるか。そのひとつに、データそのものを加工し鍵をかけ直接保護するという暗号化といった技術、またそれ以前にデータの流れをコントロールし、その流出を防ぐといったアプローチがある。そのほかにも様々な方法があるが、今回はデータの流れのコントロールについて着目し検証することとなる。本研究の検証では、オブジェクト指向モデル述語言語 UML を使いクラス図, シーケンス図を用い仕様の抽象化を行う.。次にこれらの操作を、関数型言語 ML にて記述する。この ML のプログラムを HOL 4 に渡し、システムの検証を行う。この際に、論理生成器に通すことにより ML 形式の記述で基本演算子が使えるようになり HOL 上でオブジェクト指向が使えるようになる。この検証に使用する UML：Unified Modeling Language とは統一モデリング言語であり、オブジェクト指向に基づくモデル記述を共通化したもので、オブジェクト指向分析・設計の標準表記法となっている。HOL とは公開述語論理定理証明器（システム）であり分析モデルの検証に使用することが可能である。多くのデータ型ライブラリ、および強力なデータ構築機能を備えており、システムの対象領域に存在する様々なデータ型を扱うのに適している。

目的

本研究では、組織内でのデータのセキュリティが論理的に守られていることを、定理証明により検証する。昨年までにFW：Fire Wallサーバシステムについて、ログインマネージャの検証が行われた。そこで今回は、さらにオーディットマネージャ（監査のため様々なイベントの記録を残し、TOEが監査するイベントが発生した場合監査記録を生成し、TOEのセキュアな操作を監査するために必要な情報を収集）の各機能について検証を行う。また、昨年までのHOLでの証明作業においては、大きな人的、時間的コストが必要であることも判明した、今回は、これまで通りHOLでの証明作業を行うと同時に、その作業の効率化についての研究も行う。

論文の構成

最初に形式検証について述べ、加算器について検証例を示し定理証明器HOLについて触れる。研究のメインとなるオーディットマネージャについて、その仕様とオブジェクト指向理論に基づくモデル化について述べる。さらに命題を設定し実際に検証を行う。