組織内データセキュリティの定理証明による検証に関する研究

徳田拓 (410086)

北陸先端科学技術大学院大学 情報科学研究科

2006 年 2 月 9 日

キーワード: 定理証明,HOL, オブジェクト指向, コラボレーション, 情報セキュリティ.

1 背景と目的

情報セキュリティの確立を通じ、柔軟かつ透明であり、安全・安心で高い信頼性を有する「高信頼性社会」の実現が、経済や社会の基盤として必要不可欠である。情報セキュリティとは、具体的には、秘匿性、完全性および可用性を維持するこという。ISO15408 のでは、IT セキュリティ基準のセットである、コモンクライテリア (CC) を定義している。この対象はソフトウェアに限らず、IT 製品（ソフトウェア、ハードウェア、ファームウェア）となっている。この CC が示すセキュリティ要件を元に、TOE に対するプロテクションプロファイル (PP)、セキュリティターゲット (ST) が作られ、審査され、認可される。つまり、認可を受けた ST は、セキュリティの基準を満たしている設計書であるといえる。

一方、オブジェクト設計開発法の上流過程では、UML に代表されるモデリング言語によりシステムの分析モデルが構築される。システムが要求しようを満たすことを保証することを示すための、モデル検査や定理証明などの形式検証の研究が行われている。矢竹らは、オブジェクト間のコラボレーションをベースとした証明のためのオブジェクト指向理論を、定理証明器 HOL 上で理論モジュールとして構築した。

本研究の目的は、HOL 上のオブジェクト指向理論を検証の土台とし、ST で示されるセキュリティ要求、機能要求を満たすことを証明する方法についてその可能性を示すことである。

2 研究の流れ

本研究では、FW サーバシステムの ST の存在と、オブジェクト指向理論を定理証明器 HOL 上で理論モジュール化する技術の存在を前提としている。

本研究は以下の手順で研究を進めた。

1. FW サーバシステムの ST に準ずる仕様書を想定する。
2. 仕様書を元に UML でモデル化をし、クラス図、コラボレーション図を作る。
3. モデル化したものをオブジェクト指向理論を用いて ML 形式でコード化する。
4. ML コンパイラを用いて簡単な実行テストし、コード化で起こるようなバグを取り除く。
5. コードを HOL 形式に書き直す。
6. 仕様書の内容を証明するための、システム上の述語で命題を設定する。
7. HOL 上で演繹的な手法により命題を証明する。

FW サーバシステムの ST では自然言語といくつか図表からなる。FW サーバシステム、パケットフィルタリング、識別・認証、監査の基本的機能と、それに対するアクセスコントロール機能により成り立っている。パケットフィルタリング、識別・認証、監査の基本的機能については、仕様書の内容を実現するようにモデル化し、またアクセスコントロール機能については、Role Based Access Control の概念を取り入れモデル化した。

ML 形式、HOL 形式におけるオブジェクト指向モデルは、オブジェクト指向理論を可能とする論理モジュールによって実現される。これにより、HOL 上でオブジェクト指向の概念を使用することができる。

証明では、モデルの機能が仕様書の要求を満たしているかを命題とし、証明をおこなった。これによりm証明にできない場合は、モデルがセキュリティ要求、機能要求を満たさないことを示せ、モデルの不備を指摘できる。また証明できることにより、モデルが ST で示されるセキュリティ要求、機能要求を満たすことを証明することができる。ST ので示される仕様を満たすということは、即ち、セキュリティの基準を満たしているということである。これにより、セキュリティ要求、機能要求を満たしているモデルを得ることができる。

3　研究の成果

いくつかの命題を証明し、仕様書から作ったモデルが、その命題に関して仕様書の内容を満たしていることを示した。また、一般的な、不変表明と演繹的手法以外の、命題の設定の仕方について提案をした。

4　今後の課題

ST は主に自然言語と図表などからなっている。本研究の本質的な部分は、これらの仕様書から証明すべき内容をいかに選択し、いかに論理式として表現するかである。不変表

明による命題の設定と帰納法による証明は、定理証明では一般的な方法である。しかし、これだけでは、セキュリティ要求や機能要求についての命題を作るには不十分である。今後、論理式による表現方法と証明できる内容について考えなければならない。

HOL での証明の作業は、非常に大きな人的、時間的コストを費やす。いくら理論が正しく、ST の内容について正しく証明できるとしても、非現実的なコストが必要であるならば、実用化は無理である。今後、証明をより効率的に行うタクティックについての研究、自動化の研究が必要である。