形式仕様記述（セキュリティ編）

平成２４年度シラバス

２０１２年1月１３日

国立情報学研究所

トップエスイープロジェクト

代表者　本位田　真一

1. 講座名

形式仕様記述（セキュリティ編）

2. 担当者

來間　啓伸、粂野　文洋

3. 本講座の目的

本講座では、システム検証における二つの主要技術であるモデル検査と定理証明に基づいた、セキュリティ・ポリシの検証問題を扱います。計算機システムのセキュリティは、近年ますます重視されるようになって来ました。セキュアなシステムを構成するための一般的な手法は、まずセキュリティ・ポリシを定めて何を許可するか（あるいは何を許可しないか）を明確にし、許可された振る舞いだけを実行可能にする（あるいは許可されない振る舞いの実行を阻止する）セキュリティ機構を実装する、というものです。しかし、セキュリティ・ポリシを厳密に実現したセキュリティ機構を実装することは、容易ではありません。

形式手法（Formal Methods）は、構文規則と意味規則が厳密に定められた形式仕様記述言語をデザイン記法として用いることで、曖昧性なく解釈できる記述（形式仕様）を構築します。形式仕様言語の意味規則に照らし合わせて、記述に不整合がないか、要求された特性を満たしているか、などを厳密に検証できることが長所です。また、抽象的な記述を出発点として正しさを検証しながら実装に近い記述を構築する、段階的詳細化と呼ばれる方法も提供されます。このような特徴は、厳密に記述されたセキュリティ・ポリシの正しさを検証し、セキュリティ・ポリシを強制するセキュリティ機構の正しい実装を得るうえで、有効であると期待されます。

本講座では、アクセス制御ポリシを強制するセキュリティ機構の段階的詳細化に基づく構築について、Event-B を使って学びます。Event-B は B メソッドを基盤として提案されたシステム開発手法で、詳細化の正しさを検証する方法が与えられている点に特徴があります。ここでは、ポリシを強制するセキュリティ機構の仕様を段階的詳細化によって構築するとともに、その正しさを定理証明によって検証する技術について学びます。

次に、モデル検査ツール SPIN を用いて、アクセス制御システムのモデリングと検証について演習形式で学びます。実際のシステム運用においては、様々な操作が予期されていないタイミングや順序によって実行されます。モデル検査を用いることで、全ての実行経路において満たすべきセキュリティ・ポリシが保たれていることを検証することが出来ます。この演習に先立ち、SPIN の簡単な例題演習を行うとともに、セキュアプロトコルへの検証応用等、モデル検査技術のセキュリティ分野への応用を解説します。

本講座は、設計モデル検証講座や、形式仕様記述講座において学んだ、モデル検査技術

と形式仕様記述・段階的詳細化技術を用いてセキュリティ・ポリシの検証を行うという、検証技術の集大成としての意味があります。

4. 本講座のオリジナリティ

セキュリティ機構がセキュリティ・ポリシを実現していることを、非形式的あるいは準形式的な記述を使って、厳密に検証することは困難です。一方、形式的な記述を使って検証する方法はいくつかあり、本講座においては、その代表的な二つの技術を学習する、という大きな特徴があります。本講座を学ぶことにより、これらの技術をどのような場合に適用することが出来るかという、適切な技術の適用方法について学ぶことが出来ます。

表１　従来の教材の問題点と、本講座における解

従来の教材の問題点	本講座における解
UML などの準形式的記述では、セキュリティ・ポリシがセキュリティ機構によって実現されていることを厳密に検証することは困難	形式仕様記述言語を用いることで、セキュリティ機構がセキュリティ・ポリシを実現することを仕様レベルで厳密に検証することが可能
セキュリティ・ポリシの検証に対して、単一の方法論のみを教えていた。	定理証明とモデル検査を使うことで、検証する性質により適切な技術を適用することが出来るようになる

5. 本講座で扱う難しさ

セキュリティ機構は、攻撃者からシステムを守るための盾となるため、誤りなく構成されている必要があります。セキュリティの問題では、状況に柔軟に対応できる人間が攻撃者となるため、わずかな誤りでも集中的に攻撃される可能性があるからです。したがって、セキュリティ機構はシステムの他の部分より一層堅固に構成されていることが求められます。しかし、セキュリティ・ポリシは一般に複雑であり、セキュリティ・ポリシが要求する機能をセキュリティ機構が持ち，漏れがないことを厳密に検証することは容易ではありません。本講座では、このような問題を解決する方法としての、形式仕様記述の利用について学びます。

6. 本講座で習得する技術

本講座の前半では、形式手法 Event-B について学びます。Event-B の大きな特徴は、段階的詳細化をシステム分析に利用することにあります。段階的詳細化とは、自明な、あるいは、妥当性が確認しやすい抽象的な記述をもとに、少しずつ段階的に、記述の内容を具体化・詳細化していく開発方法です。Event-B では、この詳細化の各段階で仕様の正しさを、定理証明手法を使って検証します。正しいとは、記述が矛盾していないことを意味する整合性と、下位の記述が上位の記述にしたがっていることを意味する詳細化の正当性の両方を含みます。すなわち、正しい抽象的な記述から開始して、正しさを検証しながら具体的な記述を作成します。詳細化の各段階で正しさを確認しているため、不具合が混入することがない、と期待できます。

本講座の後半では、定理証明とモデル検査というシステム検証における主要な検証技術を使った、セキュア・システムの開発技術を学習します。定理証明手法を使ったセキュア・システム開発技術では、システムが満たすべきセキュリティ・ポリシの記述から開始して段階的詳細化により設計情報を付加して、セキュリティ・ポリシを強制するセキュリティ機構の仕様を得ます。この過程を、Event-B を使って学びます。モデル検査手法に関連しては、これまで学習したモデル検査技術を用いて、アクセス・コントロール・ポリシなどのモデル化とその検証方法を学びます。ここでは、モデル検査ツール SPIN を使います。

7. 前提知識

本講座の受講生は、以下の講座を既に受講済みであることが望まれます。

- 基礎理論講座
- 形式仕様記述（基礎編）
- 形式仕様記述（応用編）
- 設計モデル検証（基礎編）
- 設計モデル検証（応用編）

次の講座を受講済みであることは、理解を深めるのに助けになります。

- セキュリティ概論
- セキュリティ要求分析

また、以下の分野に関する知識を有していることが望まれます。

- プログラミング言語論
- ソフトウェア工学
- コンピュータ・セキュリティ

8. 講義計画

第１回　形式手法概論

- 形式仕様記述と検証手法

第２回　Event-B 実習

- Event-B概論
- ツールの基本的な使い方

第３回　Event-B 実習

- Event-Bの構文

第４回　Event-B 実習

- 情報構造の表現

第５回　Event-B 実習

- リファインメント（１）

第６回　Event-B 実習

- リファインメント（２）

第７回　Event-B 実習

- 仕様記述の演習

第８回　セキュリティ・ポリシ概論

- 基本的なポリシ・モデル

第９回　Event-B による事例演習

- リファインメントによるポリシ強制

第１０回　Event-B による事例演習

- グループ討議

第１１回　Event-B による事例演習

- グループ討議

第１２回　モデル検査手法概論

- SPIN/Promela 概論
- 例題演習

第１３回　セキュリティ分野におけるモデル検査手法の適用

- セキュリティ応用概論
- モデリング演習（ドキュメント管理システムのアクセスコントロール）

第１４回　モデル検査手法による事例演習

- モデリング演習（ワークフローシステムのアクセスコントロール）
- 解説

第１５回　モデル検査手法による事例演習

- モデリング演習（セキュアプロトコルに対する適用）
- 解説

9. 教育効果

本講座を受講することにより、セキュリティ・ポリシにしたがったセキュリティ機構を形式手法に基づいて系統的に開発するための、基本ノウハウを習得できます。これらのノウハウを各々の開発現場の特性に合わせて適用することで、セキュアなシステムを強固な基盤のもとに開発することができます。

10. 使用ツール

本講座では、以下のツールを使います。

- Rodin Platform
  Event-B のための統合支援ツールであり、編集、構文検査、型検査、証明責務生成、証明支援などの機能を提供する
  http://www.event-b.org/
- SPIN
  モデル検査ツール

11. 評価

講義中に出題する課題レポートと事例演習レポートならびにグループ発表の評点、出席状況を総合して評価します。課題レポートと事例演習レポートでは、一人一人の受講者について評点を与えます。これにグループ発表の評点を加算し、出席状況と合わせて総合的に各受講者の評価を決定します。

12.参考書

（1）D. F. Ferraiolo, D. R. Kuhn, and R. Chandramouli: Role-Based Access Control, Artech House 2003.

（2）M. Bishop: Computer Security, Addison-Wesley 2003.

（3）アクセス制御に関するセキュリティポリシーモデルの調査報告書, 情報処理推進機構 2004.

（4）J.-R. Abrial: “Modeling in Event-B,” Cambridge University Press, 2010.

（5）Stouls, N., and Potet, M.-L.: Security Policy Enforcement Through Refinement Process, B2006, LNCS 4355, Springer-Verlag, pp.216-231 2006

（6）J.-R. Abrial: “The B-Book,” Cambridge University Press, 1996.

（7）J.-R. Abrial: Formal Methods in Industry: Achievements, Problems, Future, Proceedings of ICSE2006, 2006.

（8）D. F. Ferraiolo, R. Sandhu, S. Gavrila, R. Kuhn, and R. Chandramouli：Proposed NIST Standard for Role-Based Access Control, ACM Trans. on Information and System Security, Vol. 4, No. 3, pp.224-274 2001.

（9）G. Holzmann: THE SPIN MODEL CHECKER, Addison-Wesley, 2004.

（１０）来間：B メソッドによる形式仕様記述, 近代科学社, 2007.

（１１）吉岡, 青木, 田原：SPIN による設計モデル検証, 近代科学社, 2008.

その他、必要に応じて研究論文を紹介します。