

Title	モデル検査技術によるセキュリティ検証へのアスペクト指向技術の適用
Author(s)	小坂, 浩之
Citation	
Issue Date	2009-03
Type	Thesis or Dissertation
Text version	author
URL	http://hdl.handle.net/10119/8124
Rights	
Description	Supervisor: 岸知二, 情報科学研究科, 修士



モデル検査技術によるセキュリティ検証への アスペクト指向技術の適用

小坂 浩之 (0710029)

北陸先端科学技術大学院大学 情報科学研究科

2009 年 2 月 5 日

キーワード: ミスユースケース, セキュリティ, アスペクト指向, モデル検査.

本論文では, アスペクト指向技術を用いてソフトウェアのセキュリティを高めるための設計手法について議論する.

近年, ネットワークに接続する機器が増加していることもあり, ソフトウェアのセキュリティの重要性が高まっている. セキュリティ要求工学の分野では, システムにとって望ましくない状況を記述する「ミスユースケース」という考え方が研究されており, システムが持つ潜在的脅威の抽出が行われる.

このようなセキュリティの可視化に関する研究が行われている一方で, ソフトウェア工学の分野でもセキュリティ要件を充足するソフトウェアの開発手法の研究に関心が集まっている. その中で, ミスユースケースやアスペクト指向技術を扱った研究もなされている. そうした研究の一つとして, シナリオベースで設計を行い, ミスユースケースシナリオの緩和シナリオ (ミティゲーションシナリオ) をアスペクトとして定義し, システムのシナリオにウィーブするという提案がなされている.

この関連研究が提案しているシナリオベースの設計方法は, モデリングをする上で非常に理解しやすい. しかし, 設計はステートマシン図が用いられることが多いため, 関連研究はその場合の設計との親和性が低い.

そこで, 本研究ではシステムのモデルをステートマシン図で設計する手法を提案する. 提案手法の特徴は, システムモデルの記述レベルをシナリオベースからステートマシン図ベースに拡張した点である.

ここで, 関連研究が適用していた定義の中で, 本研究でも同様に適用する技術について説明する. ミスユースケース及び, ミティゲーションは関連研究と同様にシナリオで表現するものとする. また, ミティゲーションシナリオ (アスペクトシナリオ) でのポイントカットに, メッセージのシーケンスで指定する「シーケンスポイントカット」を定義していた. 本研究でも関連研究と同様に「シーケンスポイントカット」を扱うものとする. また, アスペクトシナリオの中で, どんなメッセージにも該当する「any フラグメント」を定義していた. 「any フラグメント」についても, 本研究で取り扱うものとする.

本研究では、アスペクトシナリオをステートマシン図にウィーブする手法を提案する。本手法実現のためには、アスペクトシナリオ上で指定した「シーケンスポイントカット」が指す位置が、ステートマシン図のどの位置になるのかを知る必要がある。今回は、ステートマシン図上のポイントカットの解析方法として、モデル検査器 SPIN の網羅性を用いた手法を適用する。SPIN は本来、ソフトウェアの設計の正しさを検証するためのツールであるが、その特徴は検査対象が持つ全ての状態を網羅探索することである。その特徴を利用して、SPIN にステートマシン図が取りうる全ての実行列を網羅探索させ、その中にシーケンスポイントカットのメッセージ列があるかを検査する。SPIN に入力可能なモデルは Promela 言語であるため、ステートマシン図を Promela に変換する処理を行う。この処理に関しては手動で行った。

提案する手法によって、アスペクトシナリオ上のポイントカットが指す位置が、Promela 上のどの位置に当たるかを解析することが出来た。この Promela 上のポイントカットに対して、アスペクトシナリオのウィーブ処理を行う。

ここで Promela へのウィーブをサポートしている Aspect Promela ツールを適用する。Aspect Promela は本研究室の OB である大野が作成したツールである。SPIN によるステートマシン図の実行列の解析～Aspect Promela の適用までを、本研究で提案するウィーブとする。

提案手法の有効性を評価するために、電子投票システムの例題に本手法を適用させた。投票を行うシステムと、システムの脅威のシナリオを用意し、脅威を緩和するシナリオを提案するウィーブ手法でシステムにウィーブした。その結果、アスペクトシナリオが指定した箇所(想定した箇所)に適切にウィーブされたことを確認した。また、ウィーブ後のシステムが脅威を防ぐ設計になったことを検証実験により確認した。