

安全・安心を設計する



SSE Project: 安全・安心なソフトウェアを構築するための研究プロジェクト

吉岡信和、総研大、早稲田大学、信州大学、JAIST、情報セキュリティ大学院大学、オープン大学、フロリダアトランティック大学、イーストロンドン大学ほか

どんな研究？

近年、個人情報流出や不正アクセスの危険性など、情報システムのセキュリティは社会問題となってきました。その中で、アドホックなセキュリティパッチや運用強化などの対応は限界があります。本プロジェクトでは、システムの**要求時から運用まで一貫したセキュリティ**を考慮した開発を実現します。

何ができる？

安全・安心なソフトウェアの構築をサポートするためのソフトウェア工学技術を確立し、その普及を目指します。具体的には下記を開発します。

- 体系的な方法論の確立
- モデリングをサポートするツールの開発
- セキュリティソフトウェア工学の教育教材開発

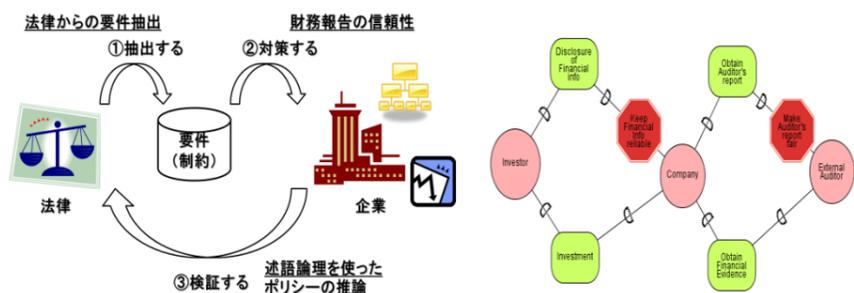
プロジェクトの目的

安全・安心なシステムを構築するためのセキュリティ・セーフティのモデル化・インテグレーション技術の開発

要求: 法律を順守するためのフレームワークの研究

by JAIST 河本 高文

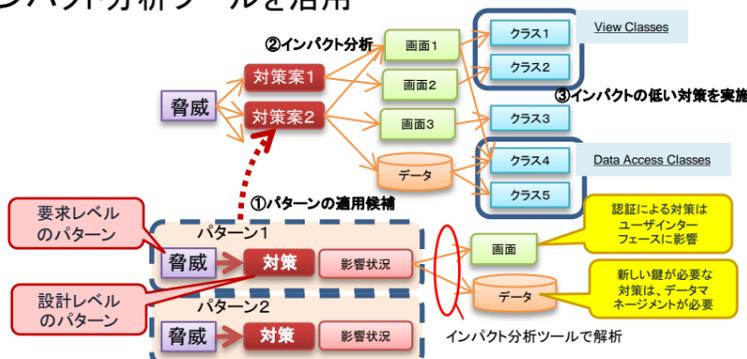
<背景>: 個人情報保護法、内部統制、国際会計基準などの新しい法律や基準への迅速な対応が必要。
 <方法>: 法律から要件を抽出、要件に沿った対策を設計、妥当性を検証。要件は、ゴール指向言語でモデル化。



設計: セキュリティのインパクト分析手法の研究

joint work with 信州大学

<目的>: セキュリティ変更時のコストを予測、適切な対策を選択
 • 要求レベルと設計レベルのセキュリティパターンの体系化
 • インパクト分析ツールを活用



実装: Agile開発におけるセキュリティ対策の研究

by 総研大 宗藤 誠治

<目的>: セキュリティ対策のコスト低減と品質向上

<課題>: Agile開発におけるセキュリティ確保

- 1) Agile開発のスピードに、既存のセキュリティ対策手法はついていけない(軽量な手法が必要)
- 2) 様々な脅威と脆弱性への網羅的な対応が必要(自動化)

<解決>: セキュリティ機能を表現する抽象モデルの利用

- 1) 抽象モデルはソースコードから自動生成
- 2) コード中心の開発と並行して、抽象モデル上でのセキュリティ分析、テスト生成が実施できる
- 3) セキュリティ機能の配置をモデル上で確認できる
- 4) 実行可能なアクセプタンステストを生成
- 5) テスト駆動設計との高い親和性

Ruby on Rails に対応したツールを公開中
 URL <https://github.com/munetoh/railroadmap>

