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、田口研治、久保淳人、本位田真一、
早稲田大学、電通大学、東工大学、信州大学、立命館大学、JAIST、
富士通研究所、みずほ情報総研、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

なにができる？

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

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ています。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。

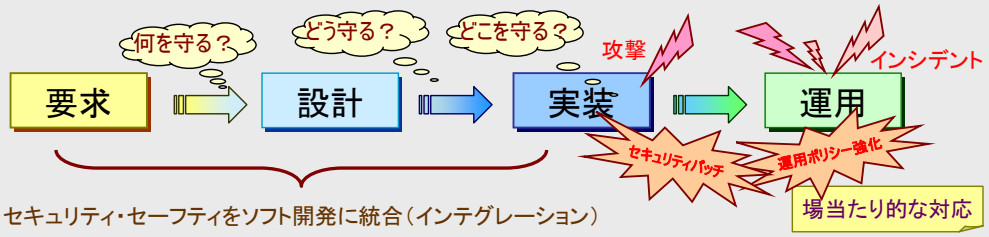
背景

- インターネットの発展、情報システムのライフライン化
- セキュリティは現代社会に多大の影響：情報流出、不正アクセス

課題

情報システムのセキュリティを高める技術は不十分
ほとんどの研究は、基礎アルゴリズム・プロトコル、あとは運用でカバー

➔ セキュアなシステムを開発するための**体系的な方法論**が必要



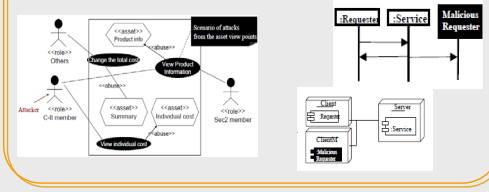
プロジェクトの目的

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・普及

具体的な研究例

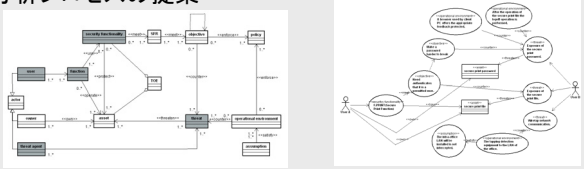
セキュリティパターンの研究

- アタックのモデリング・パターン化
- パターンの形式化
- パターンの摘出・検索



コモンクライテリアに基づく開発方法論の研究

- セキュリティの関心毎をSTに基づき整理、メタモデルを提案
- ユースケースを拡張したモデル：
  ユースケース＋資産、脅威、対策、前提
- 分析プロセスの提案

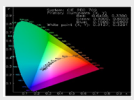


セキュリティ要件と設計のトレーサビリティに関する研究

- セキュリティ目標・要件と設計、
  脆弱性・対応関係をモデル化
- ビジネスとシステムを切り分けた開発プロセス

セキュリティの可視化

- セキュリティメトリクスの規定
  システムの危険性、安全性の数値化
- 効果的な表示モデル



その他

- 内部統制に基づくシステム開発方法論の研究
- セキュリティ教材の開発
- 無線センサーセットワークのセキュリティ技術