安全・安心なサービスを作る

SSE Project: 安全でプライバシーに優しいソフトウェア構築に関する研究プロジェクト

共同研究：早稲田大学、神奈川大学、情報セキュリティ大学院大学、東京学芸大学
オープン大学、フロリダアトランティック大学、アイルランドソフトウェア工学研究所ほか

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ています。その場しのぎのセキュリティパッチや運用強化などでは限界があります。
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とプライバシー**を考慮した開発を実現します。

何がわかる？

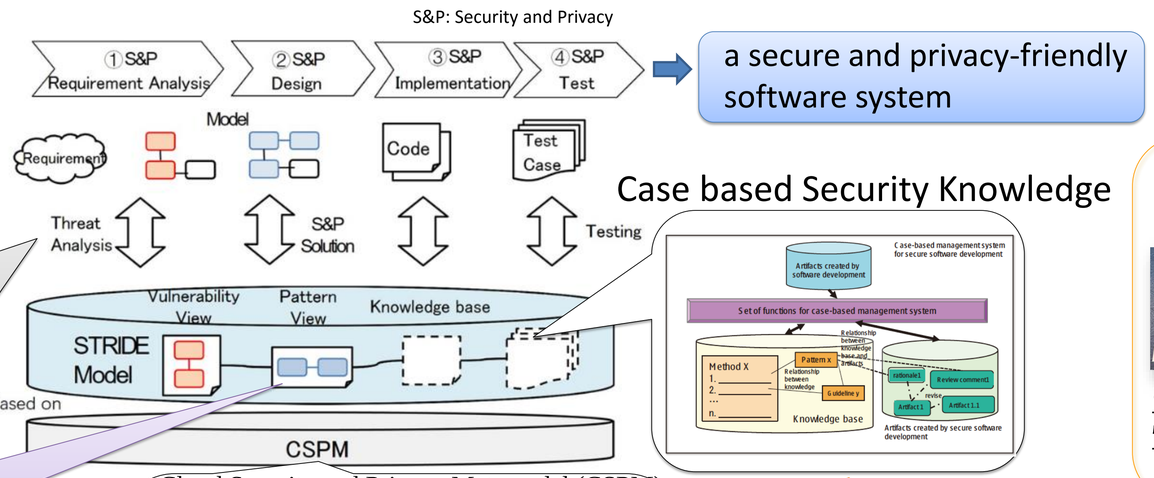
安全・安心なソフトウェアの構築をサポートするためのソフトウェア工学技術を確立し、その普及を目指します。具体的には以下を開発します。

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

安全・安心なシステムを構築するための
セキュリティとプライバシーのモデル化・インテグレーション技術の開発

研究テーマ例

全体像

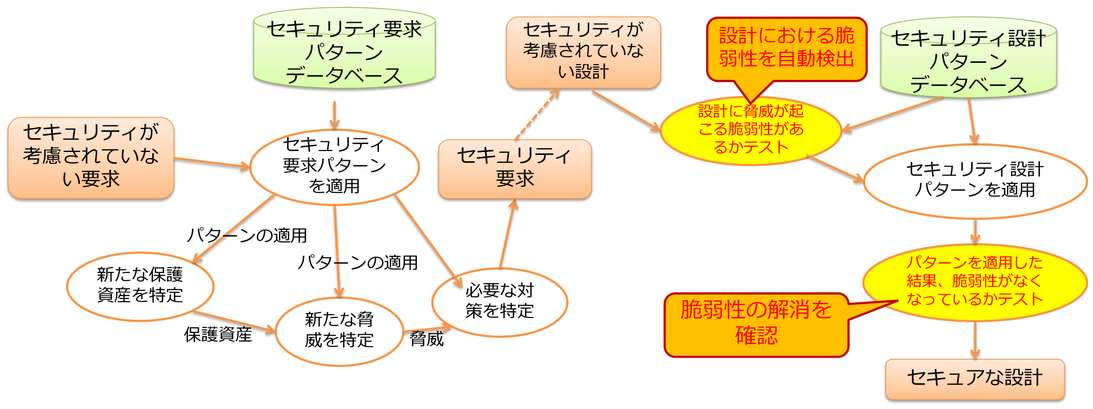


セキュリティパターンの例
シングルアクセスポイントパターン
Markus Schumacherほか, "Security Patterns: Integrating Security and Systems Engineering", Wiley,2006.

セキュリティ開発に必要な概念の整理

セキュリティパターンに関する研究

<背景>
セキュリティパターンは専門家以外がセキュリティを考慮した開発を行うのには有用。間違った適用は新たなセキュリティの脆弱性になりうる
<方法>
開発中のソフトウェアにセキュリティパターンを適用する必要があるか、また、適切にパターンを適用したかをテストにより確認



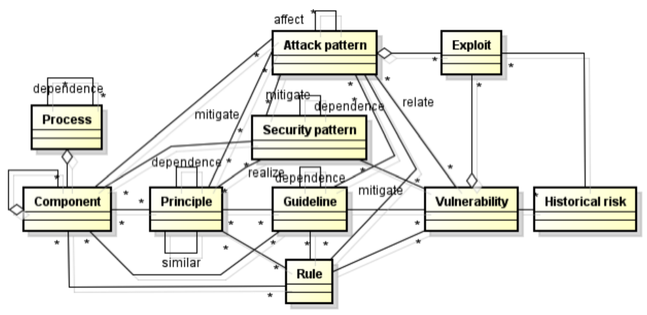
透明性を利用した人的セキュリティリスクの軽減

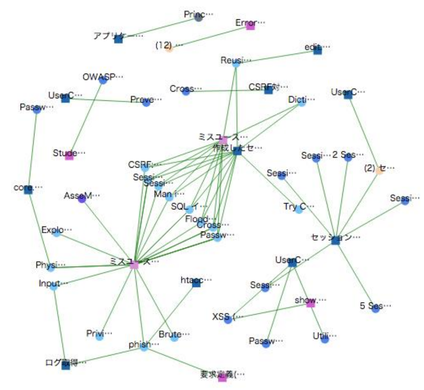
モニタリングの透明性による注意喚起例

<背景>
内部犯や不注意によるセキュリティインシデントが社会問題
<方法>
- セキュリティに関する情報を利用者や攻撃者に適切な粒度・情報量で見える化（透明化）
- 望ましくない行動の軽減

オントロジーを用いたセキュリティ設計

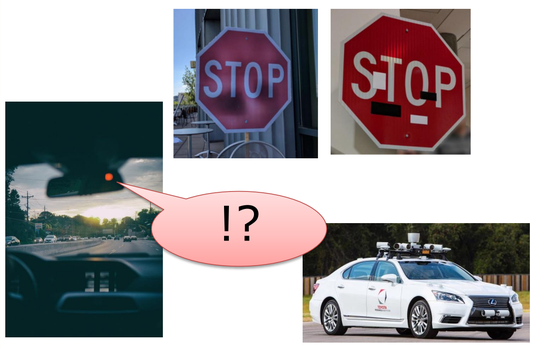
<背景>：セキュリティは様々な概念やガイドラインがあり、技術を習得するのが難しい
<方法>：セキュリティ知識とセキュアなソフトウェア開発で作成される成果物との関連などをセキュリティ知識を整理し、その適用事例や典型例から効率よく技術を学べる手法を提案





機械学習システムのためのセキュリティ設計 NEW

誤認識する書き換え例[1]



[1]Eykholt, K., Evtimov, I., Fernandes, E., Li, B., Rahmati, A., Xiao, C., ... Song, D. (2017). Robust Physical-World Attacks on Deep Learning Models.

<背景>
機械学習は様々なシステムで活用されているが、セキュリティの問題が発生する可能性。特に自動運転ではセキュリティは重大な問題
<研究課題>
- 訓練データ・センサーデータの悪意のある書き換えの自動検知
- 学習モデルの脆弱性の排除
- 機械学習モデルとプログラムとの組み合わせによるフェールセーフ設計

NII
連絡先：吉岡信和／ 国立情報学研究所 アーキテクチャ科学研究系
TEL：03-4212-2570 FAX：03-4212-2697 Email：nobukazu@nii.ac.jp