

# セキュリティシリーズ

講師陣(予定):

- 戸田 洋三(JPCERT コーディネーションセンター)
- 福本 郁哉(JPCERT コーディネーションセンター)
- 萱島 信(日立製作所)
- 川岸 敏之((株) ECSEC Laboratory)
- 金子 朋子(創価大学)
- 大久保 隆夫(情報セキュリティ大学院大学)
- 松崎 和賢(中央大学)
- 河本 高文(元東芝)
- 吉岡 信和(早稲田大学/NII)

# セキュリティシリーズが目指す人材像

## 【背景】

- インターネット上のあらゆるサービスがサイバー攻撃の対象になりえる。

## 【目標】

- 必要十分なセキュリティを担保したソフトウェアシステムを開発できる能力を持つ
  - 先進的な技術を使ってセキュリティを担保できる
  - 適切なセキュリティ要件、設計、実装、運用設計ができる
  - (基礎) **既知の脅威や脆弱性**に対して適切かつ迅速に対処できる。よく知られたセキュリティの脆弱性を排除したソフトウェアを開発できる。
  - (先端) **まだ明らかになっていない、知られていない脅威や脆弱性**を迅速に発見し、適切に対応できる。**複雑なセキュリティ要求**を適切に規定できる。

# セキュリティシリーズの講座

(基礎)

すべてのソフトウェアエンジニアが知っておくべきセキュリティの基本的な知識とスキル

- セキュアプログラミング
- セキュリティの脅威分析実践演習

(先端)

今後重要になる知識とスキル

- セキュリティとセーフティの要求分析

※講義間に依存関係がないので、特定の講義のみの受講でも問題ありません

# セキュアプログラミング

## 【扱うトピック】

- Webアプリケーションのセキュリティ
  - Webの脆弱性と診断
  - Webのセキュアプログラミング
- 演習：脆弱性の確認とその対策のための修正

## 【前提知識】

Webシステム構築法の概要、Webアプリ構築のためのプログラミング言語(PHP, JavaScript, etc.)を知っていることが望まれる

# セキュアプログラミングのシラバス

第1回 セキュリティ入門(座学)

第2回 脆弱性概論とWebの仕組み、Web脆弱性(座学)

第3回 Web脆弱性と攻撃の仕組み(座学)

第4回 Web脆弱性の確認方法とセキュアプログラミング(座学)

第5回 Web脆弱性の確認方法とセキュアプログラミング(演習)

第6回 ツールを使った脆弱性検査(座学)

第7回 ツールを使った脆弱性検査、報告書作成(演習)

# セキュリティの脅威分析実践演習

## 【扱うトピック】

- システムのセキュリティ脅威の分析
  - IoTシステムのセキュリティ
  - 5つのW(Where、Who、When、Why、What)に基づく脅威の洗い出し
- 演習中心

# セキュリティの脅威分析実践演習のシラバス

第1回 セキュリティの脅威分析概論

第2回 セキュリティの脅威分析の演習(前半1)

第3回 セキュリティの脅威分析の演習(前半2)

第4回 コモンクライトリアによるセキュリティ要求の保証

第5回 IoTセキュリティ概要

第6回 セキュリティの脅威分析の演習(後半1)

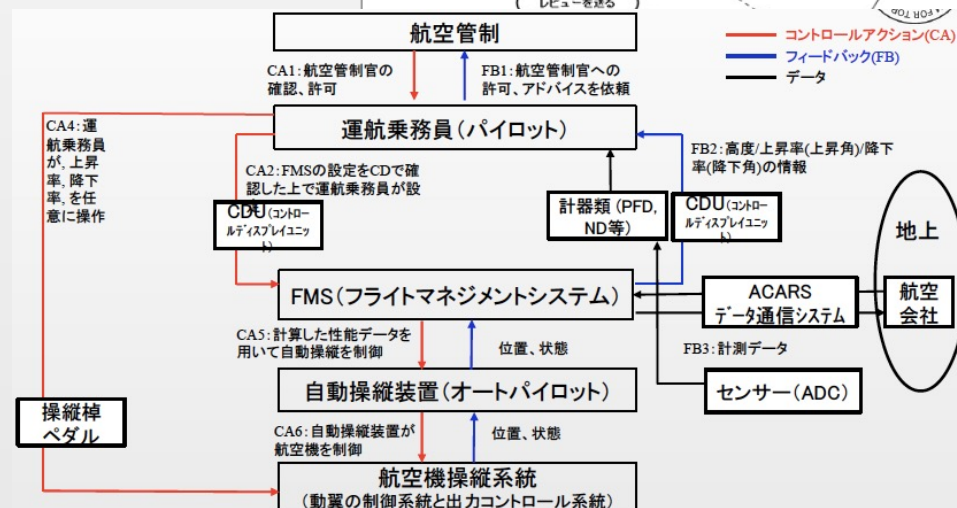
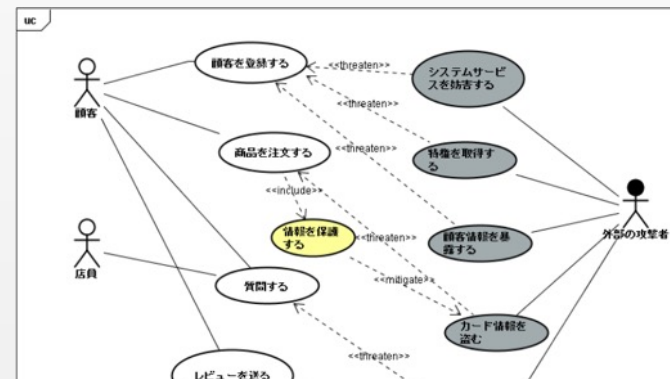
第7回 セキュリティの脅威分析の演習(後半2)

# セキュリティとセーフティの要求分析

■ セーフティやセキュリティに関する適切な要求を抽出する方法を学ぶ.

■ ハザード分析手法: STAMP、  
ミスユースケース

■ リスク分析手法





# セキュリティとセーフティの要求分析のシラバス

- 第1回 機能安全入門
- 第2回 STAMP/STPAによる安全分析基礎
- 第3回 セーフティ2.0、レジリエンスエンジニアリング等の新たな安全分析の概要
- 第4回 ミスユースケースを用いたセーフティとセキュリティの脅威分析概論
- 第5回 STAMP/STPAによる安全分析演習(1)
- 第6回 STAMP/STPAによる安全分析演習(2)
- 第7回 ミスユースケース等を使った脅威分析の演習