



# 大久保研究室



指導教官 大久保 隆夫

専門 システムセキュリティ、SbD (Security by Design)、脅威分析

著書 イラスト図解式この一冊ですべてわかる セキュリティの基本 SBクリエイティブ出版

## セキュリティ・バイ・デザイン

セキュリティ・バイ・デザインとは… *SbD : Security by Design*

企画・設計段階から情報セキュリティ対策を組み込むこと



IoT機器などの組み込み機器、自動車がしばしばハッキング対象としてとりあげられ、IoTや組み込み機器に対するセキュリティ脅威が高まっている。そのため、開発者は従来のセーフティ系ハザード、リスク分析の他に、セキュリティのリスク分析も行うことが求められている。

### システム・ソフトウェアを、はじめから安全につくる!

### SbD手法

脅威分析を誰でもできるようにするには?

- Attack Treeの効率的分析

Attack Treeが正しいか評価できる? また、機械的に改善できるか?

- Attack Treeの評価、リファクタリング

アジャイルとセキュリティの相性が悪い

- DevOpsをセキュアにする技術

運用→開発の流れでセキュアにできるか

### SbDを実現する技術

#### マルウェア攻撃解析

コードの類似性でマルウェアを特徴づけできないか?

- コールグラフの類似度を用いたマルウェア分類
- シンボリック実行を用いたマルウェア解析妨害の回避
- 不正APの検知
- 攻撃者の識別、fingerprinting

解析妨害機能をいかに回避するか

#### システム防護技術

- IoTセキュリティ
- AIのセキュリティ
- 車載セキュリティ
- 制御系セキュリティ
- Webセキュリティ
- ゲームのチート対策
- ロボットOSのセキュリティ
- 衛生システムのセキュリティ

所属学生 博士課程前期 14名  
博士課程後期 2名

毎週火曜5限ゼミ開催  
定期的な個人指導の保証

秋/春合宿  
CTFサークル活動