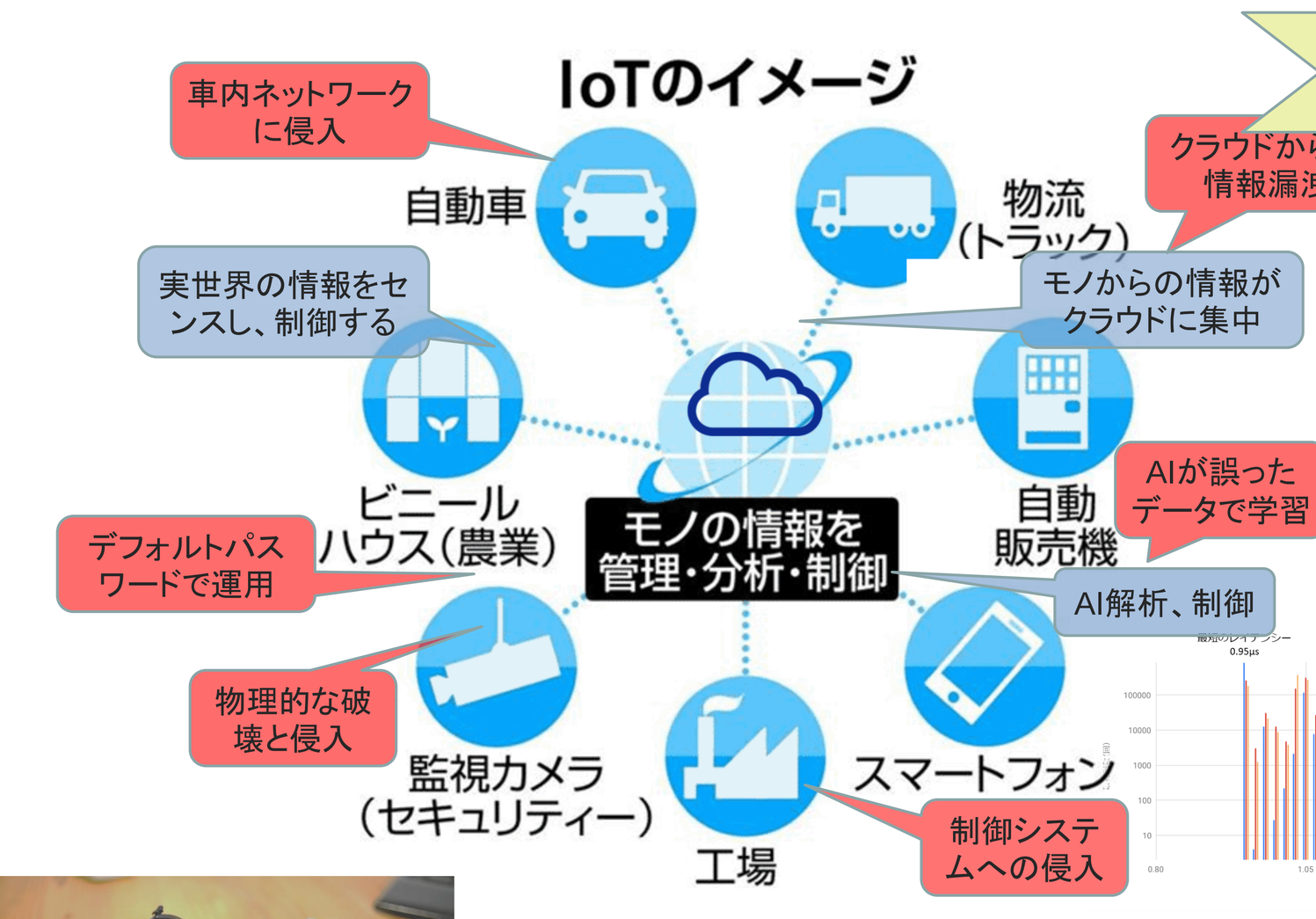
松井研究室

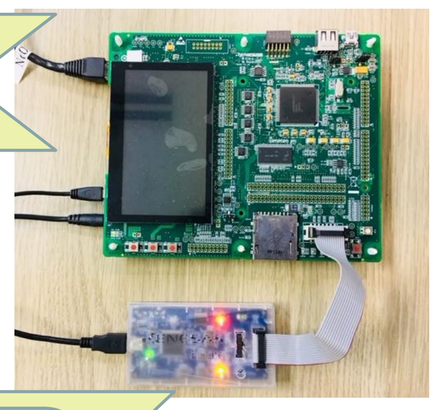
明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

IoTとAIのセキュリティを守る

ウェアラブル，スマートホーム，自動車，産業機器などさまざまなモノがインターネットにつながるIoTが進行しています．もともと独立した使用を想定していた機器がインターネットにつながると、新たなセキュリティリスクが生じます。PCやスマフォなどのパーソナルIT機器と大きく異なるのは、これらのIoTデバイスは、M2M（機器間通信）で動作するので、ユーザーのパスワードでは保護できないことです．デバイスが公共の場所に置かれるため、物理的な攻撃にもさらされます．たとえば、デバッグポートからデータを抜き取って、プログラムを改竄したり、機器になりすますことが可能です．IoTには，AIが組み込まれ，自動運転等への応用が見込まれていますが，AIに対する敵対的サンプル攻撃が問題視されています．松井研究室では、これらのIoTとAIのセキュリティを研究しています．

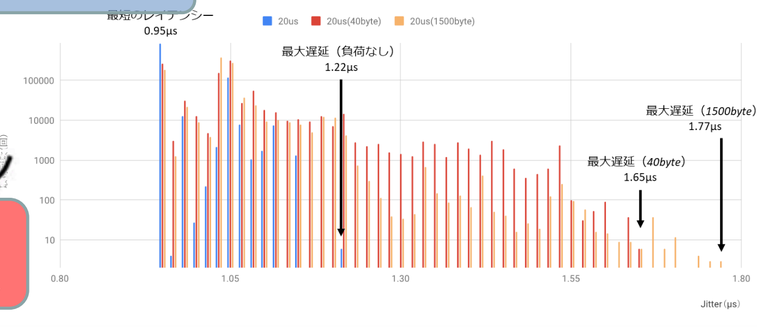
2020年1月発刊

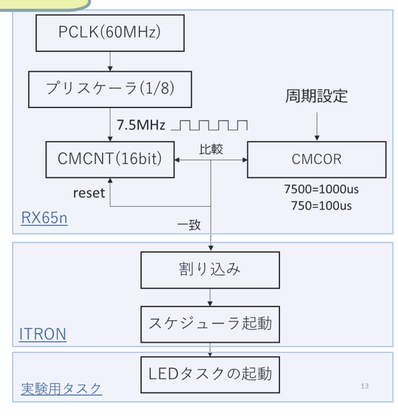


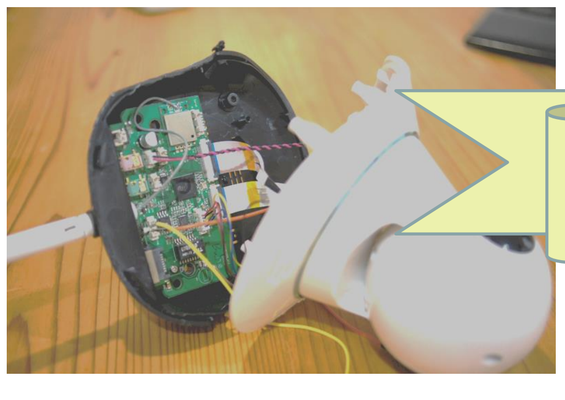


MCUのハードウェアセキュリティ機能

RTOSのリアルタイム性能評価



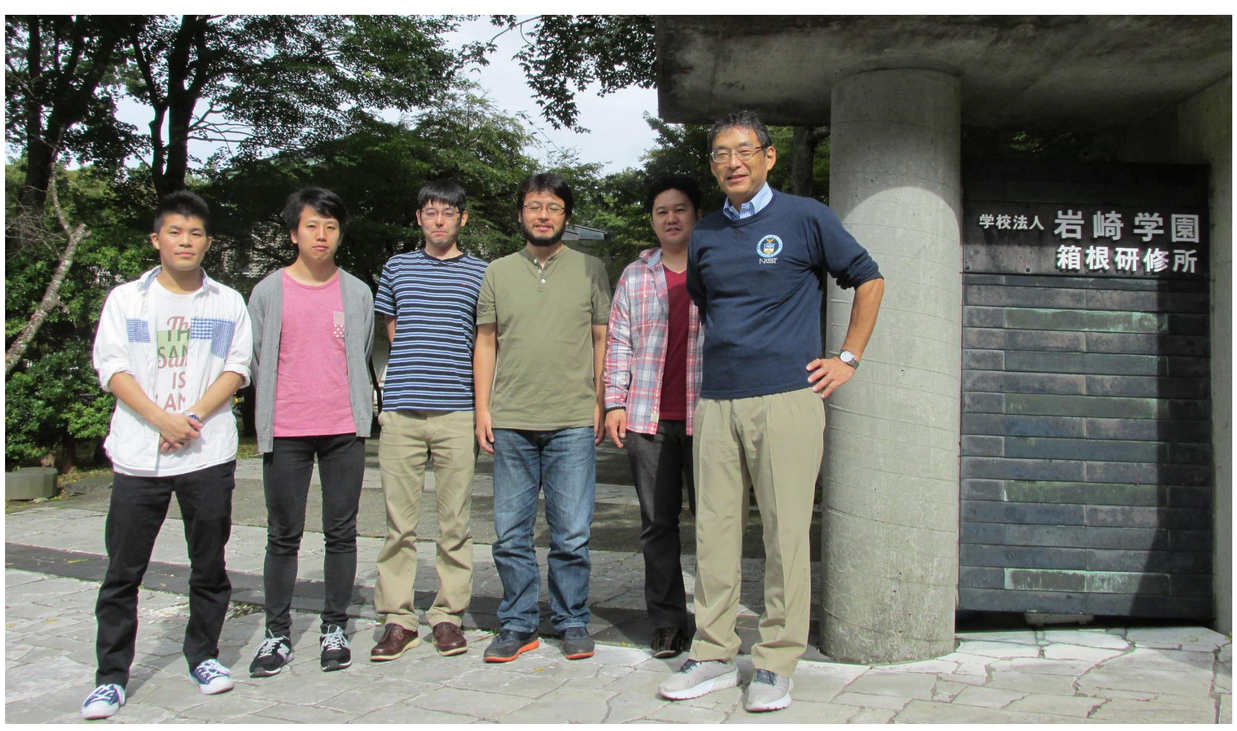




IoTデバイスのリバースエンジニアリング

松井研究室　2017-2020年の研究成果

- 脆弱性検査ツールの評価
- PUF（LSIの指紋）の信頼性評価
- センサーネットワークの発信源隠蔽法
- 鉄道制御システムへのセキュアOSの適合性評価
- 加速度センサーLSIへの超音波誤動作誘発攻撃への対策法
- リアルタイムOSのネットワーク負荷攻撃耐性評価
- ■ モバイルネットワークの発信源探索法(D)
- IoTへのセキュリティ攻撃の動向調査
- ■ AIへの敵対的サンプル攻撃に対する画像処理による防護法(D)
- 人間の視覚特性に合わせたノイズの目立たない敵対的サンプル生成法
- IoTマルウェアの発するコマンドの概念ドリフト検出
- 車載ネットワークの多層ログアーキテクチャ



教授紹介　松井俊浩：　1982年から、電子技術総合研究所において、ロボットの動作計画、オブジェクト指向を用いたロボットプログラミング、オフィス内移動サービスロボットJijo2などの研究。1990年代に、スタンフォード大学、マサチューセッツ工科大学、オーストラリア国立大学などの客員研究員。2003-2007年、産総研デジタルヒューマン研究センター副センター長としてヒューマノイドロボットの実時間制御、身体バイタルサインから心理状態の推測の研究。2012年から産総研セキュアシステム研究部門長、2015-2017年、NEDOにおいてIT技術開発戦略の策定、2016年より本学教授。授業は、情報デバイス技術、プログラミング、情報システム構成論、実践的IoTセキュリティを担当。