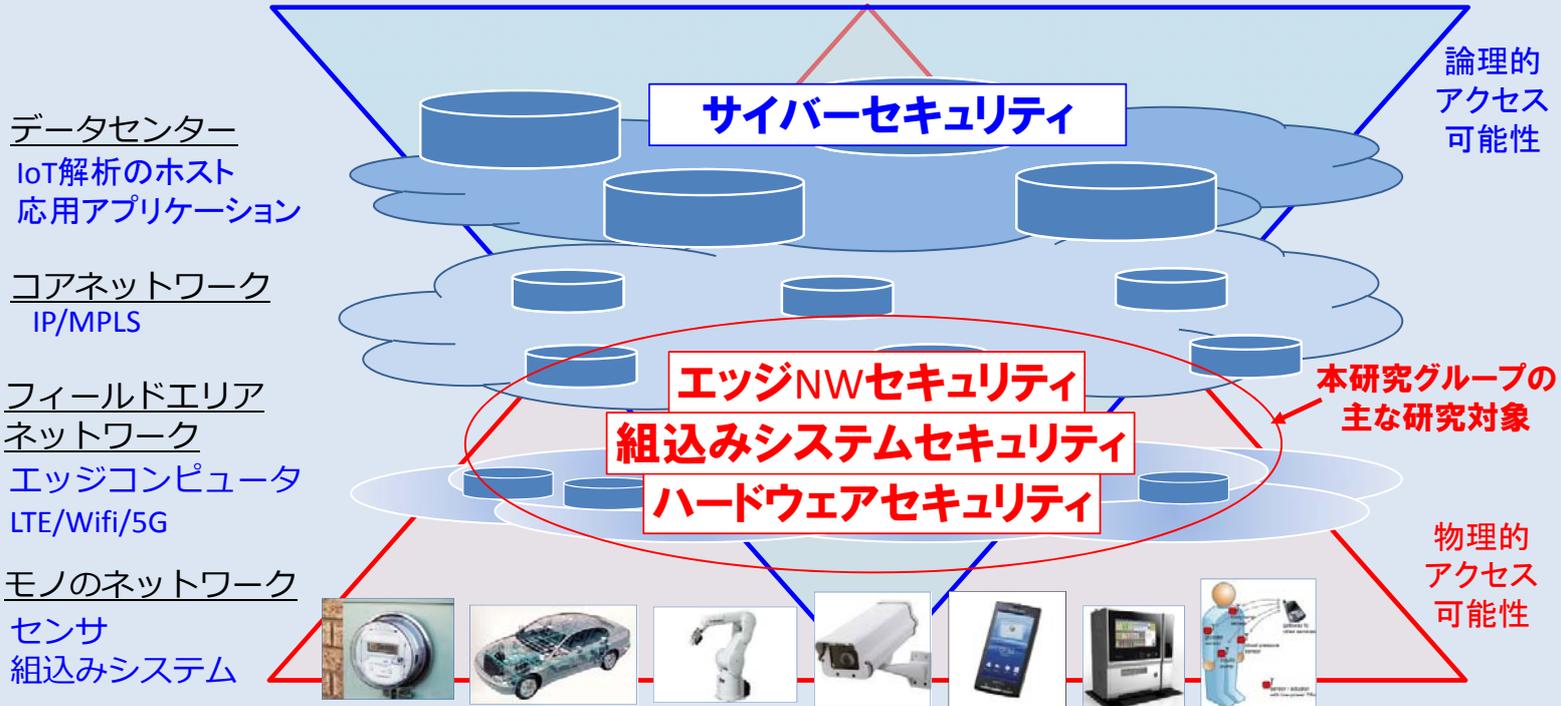


Society5.0を支えるハードウェアセキュリティ技術

スタッフ: 本間尚文教授, 上野嶺助教, Ville Yli-Mäyry特任助教

研究対象

IoTやCPS等の次世代情報通信技術の情報セキュリティ技術, 特に, 膨大かつ多様な情報発生源(センサ端末)のレベルからシステムの安全性・信頼性を担保するサイバーフィジカルセキュリティ技術を対象とする



研究テーマ

1) 暗号等に基づくセキュリティコンピューティング, 2) 各種物理攻撃(システムに物理的にアクセスして行う攻撃)に対する頑健なセキュリティシステム, 3) 利用環境や応用分野を考慮した情報通信システムのセキュリティ設計・評価を主な研究テーマとして取り組んでいる. 将来的には, ハードウェアアルゴリズムからシステム実装, 環境・応用までを系統的に統合したシステムセキュリティ設計・評価技術の確立を目指している.

セキュア情報システム構築技術

セキュリティ分析・評価技術

次世代・現代暗号のLSIコンピューティング

セキュリティシステム構築技術

各種物理攻撃・防御理論と実証

情報・電磁環境を考慮した情報セキュリティ

スマートシティ パブリックインフラ ヘルスケア オートモーティブ エナジ リテール

CRYPTREC
Cryptography Research and Evaluation Committees

NIST

応用に最適化したセキュリティ・バイ・デザイン

標準化の推進