

情報・物理セキュリティ 研究拠点

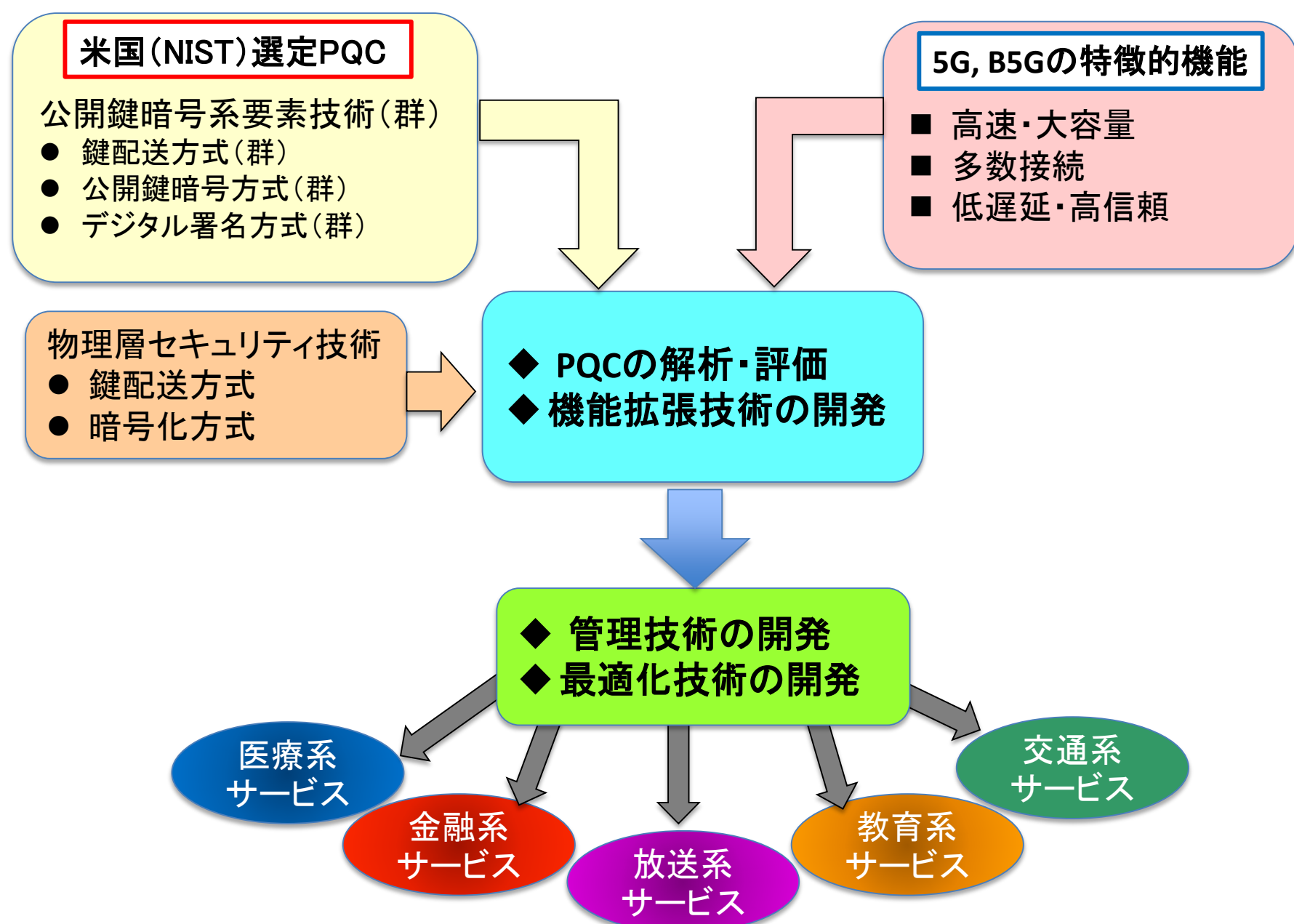
サイバー攻撃等に対抗する情報・物理セキュリティの未解決問題への挑戦

最先端暗号技術、ソフトウェア・ハードウェアセキュリティ技術、ネットワーク・システムセキュリティ技術等の研究を進展させ、IoT時代における情報・物理セキュリティの未解決問題に挑戦する。

研究内容

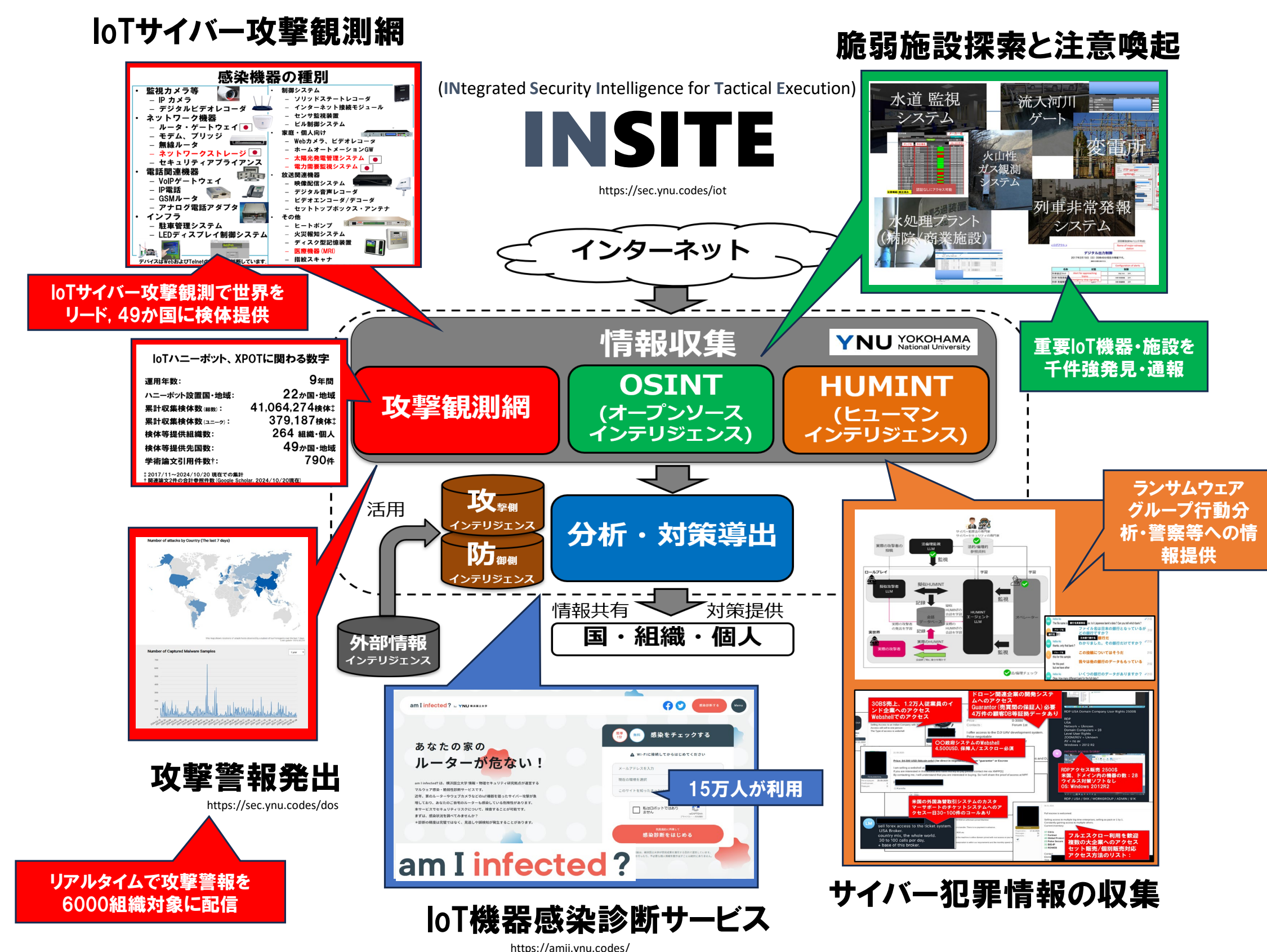
◆次世代暗号技術の研究

耐量子計算機暗号（PQC: Post-Quantum Cryptography）や高機能暗号の研究開発、およびそれに必要な数理基盤を発展させ、次世代暗号技術の開発と成果の社会展開（国際標準化等）を行う。



◆サイバーセキュリティ技術の研究

サイバー攻撃の観測・分析・対策や、近い将来に発生が予想される攻撃の予測など実践的で実用性の高いサイバーセキュリティ技術の研究開発と成果の社会展開（社会実装）を行う。



活動実績

◆2024年度

- 論文(査読有)：29篇
論文誌：18篇，国際会議：11篇
- 受賞数：11件
- 社会貢献
国際標準化寄書提出：2件
セキュリティ脆弱性報告：4件

◆2025年度

- 論文(査読有)：16篇
論文誌：4篇，国際会議：12篇
- 受賞数：6件
- 社会貢献
国際標準化寄書提出：1件
セキュリティ脆弱性報告：2件

外部資金

- ◆2024年度：約4億円
- ◆2025年度：約4.5億円

