# 人工知能（AI）が浸透するデータ駆動型の経済社会に必要なAIセキュリティ技術の確立

【最大25億円程度】

- 人工知能（AI）の技術は、民生部門・公的部門において着実に活用が広がり、**広範な産業や社会インフラなどに大きな影響**を与えている。
- しかし、AIそのものを守るセキュリティ（Security for AI）に関する脆弱性は、国際的にもまだ**十分に理解されていない**。また、AIを活用したサイバーセキュリティ対策（AI for Security）については、製品やサービスの商用化が進む一方、**年々複雑化・巧妙化するサイバー攻撃に対処**することが求められている。
- これらの課題に対応するため、産学官の技術力向上を図ることを目的として、**AIセキュリティ（Security for AI 及びAI for Security）に関する必要な知見蓄積や、知識・技術体系の整理・獲得**を目指す。

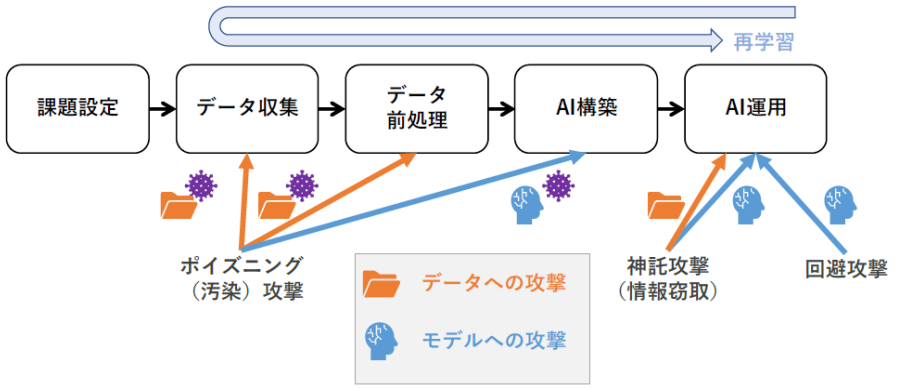
## 1 Security for AI

AIを守るための機密性・完全性・可用性の確保や、AIが攻撃された際の社会的影響への対応に関する研究開発の方向性を整理し、AIが活用された具体的なシステムを対象として、防御技術のプロトタイプの開発・実証を目指す。

## 2 AI for Security

具体的なシステムを対象として、最先端の攻撃技術に対する革新的なAI活用によるセキュリティ技術のプロトタイプの開発・実証を行うほか、仮想システムにおいて攻撃・防御を行う模擬対戦による技術の高度化と人材育成、コミュニティ拡大を目指す。

**AIモデルへの脅威とAIライフサイクルの関係（イメージ）**




出典：（独）情報処理推進機構、セキュリティ関係者のためのAIハンドブック（2022年８月）

**支援対象となる技術** ▶AIセキュリティに係る知識・技術体系