文部科学省

資料４

# 文部科学省の研究開発関連の取組

2022年9月

文部科学省 研究振興局

# AIP: Advanced Integrated Intelligence Platform Project
# 人工知能/ビッグデータ/IoT/サイバーセキュリティ統合プロジェクト

令和5年度要求・要望額　11,134百万円
（前年度予算額　10,862百万円）
※運営費交付金中の推計額含む

文部科学省

## 背景

○「AI戦略2022」（2022年４月）及び「統合イノベーション戦略2022」（2022年６月）に基づき、AI等の最先端の基盤的技術の研究開発、社会実装等の総合的な取組を官民一体となって推進。

**【AI戦略2022（令和４年４月22日　統合イノベーション戦略推進会議決定）】**
○理研AIP は、AIに関する理論研究を中心とした革新的な基盤技術の研究開発で世界トップを狙い、（中略）、各AI関連中核センターはその研究成果を迅速に社会で活用させることを目指すことを目標とし、AI研究開発に取り組んできた。これらの取組は、日本が先端的AI技術を構築していくために必須なものであり、今後も注力していく。そして、日本が世界と伍していくべく、AI研究開発の日本型モデルを創造し、世界の研究者から選ばれる魅力的なAI研究拠点化を実現していく。さらには、そのような環境の中で、日本がリーダーシップを取れる先端的AI技術を世の中に生み出していく。

**【統合イノベーション戦略2022（令和４年６月３日　閣議決定）】**
○AIの社会実装の更なる推進のため、画像認識、自然言語処理等での広範かつ効果的な活用が期待されるディープラーニングを重要分野として位置付け、企業による実装を念頭に置きつつ、AIの信頼性向上、AI利活用を支えるデータの充実、AIを巡る人材や技術情報、データ取扱いルール等の追加的な環境整備、政府におけるAI利活用の推進、我が国が強みを有する分野とAIとの融合に力点を置いて取り組む。

## 事業概要

○ 世界最先端の研究者を糾合する拠点として、**理化学研究所にAIPセンター**を設置し、AI、ビッグデータ、IoT、サイバーセキュリティに関する革新的な基盤技術の研究開発を進めるとともに、**JSTのファンディングを通じた全国の大学・研究機関等のAI関連の研究支援**を**一体的に推進**。

### 革新知能統合研究センター　（AIPセンター）
理化学研究所【拠点】

国 →（補助金）→ 理化学研究所

要求・要望額：3,801百万円（3,249百万円）
事業期間: 2016～2025年度

- **世界最先端の研究者を糾合**し、革新的な**基盤技術の研究開発**や我が国の強みである**ビッグデータを活用した研究開発**を推進。

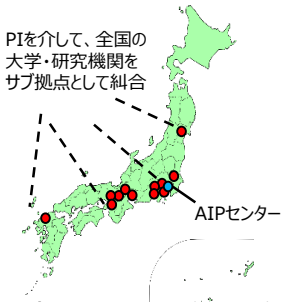
汎用基盤
① **深層学習の原理の解明**、現在のAI技術では対応できない高度で**複雑・不完全なデータ等に適用可能な基盤技術**の実現 等

目的指向
② 日本の強みを伸長:AI×**再生医療・モノづくり 等**
社会課題の解決:AI×**高齢者ヘルスケア・防災 等**

倫理社会
③ AIと人間の関係としての**倫理の明確化**
AIを活かす**法制度の検討 等**


#### 理研AIPセンターにおいて今後強化する取組

AIPセンター全体で、**従来の深層学習を超える、信頼性の高い次世代のAI基盤技術の理論構築から社会実装**の一気通貫プログラムを形成
✓深層学習理論の完成により、**我が国における深層学習の応用を大きく加速**
✓従来の深層学習を超える、**説明可能なAI(XAI)等の次世代AI基盤技術の新たな潮流を創出**し、次フェーズのAIの社会実装において我が国を世界のトップランナーへ




全36チーム／ユニット、594名
（令和４年４月時点）

一体的に推進

### 戦略的創造研究推進事業　（一部）
科学技術振興機構【ファンディング】

要求・要望額：7,332百万円（7,613百万円）※
※運営費交付金中の推計額

- AIやビッグデータ等における**若手研究者の独創的な発想**や、新たなイノベーションを切り拓く**挑戦的な研究課題**を支援。
- **「AIPネットワークラボ」としての一体的運営**により、課題選考から研究推進まで幅広いフェーズでの**研究領域間の連携**を促進。

令和４年度の JST AIPネットワークラボ 構成領域

**CREST**
- 基礎理論とシステム基盤技術の融合によるSociety 5.0のための基盤ソフトウェアの創出（岡部総括）
- データ駆動・AI駆動を中心としたデジタルトランスフォーメーションによる生命科学研究の革新（岡田総括）
- 信頼されるAIシステムを支える基盤技術（相澤総括）
- 数学・数理科学と情報科学の連携・融合による情報活用基盤の創出と社会課題解決に向けた展開（上田総括）
- 人と情報環境の共生インタラクション基盤技術の創出と展開（間瀬総括）
- イノベーション創発に資する人工知能基盤技術の創出と統合化（栄藤総括）

**さきがけ**
- 文理融合による人と社会の変革基盤技術の共創（栗原総括）
- 社会変革に向けたICT基盤強化（東野総括）
- 信頼されるAIの基盤技術（有村総括）
- IoTが拓く未来（徳田総括）
- 数理と情報科学で解き明かす多様な対象の数理構造と活用（坂上総括）
- 人とインタラクションの未来（暦本総括）

**ACT-X**
- AI活用で挑む学問の革新と創成（國吉総括）
- 数理・情報のフロンティア（河原林総括）

国 →（運営費交付金）→ JST →（委託）→ 大学・国立研究開発法人等

※ 令和５年度からAIPプロジェクトに親和性の高い新規領域が発足した場合、追加でAIPネットワークラボに参画する可能性あり。

# AIPセンターのこれまでの成果（サイバーセキュリティ関連）

## 敵対性サンプル（Adversarial Example, AE）によるAIの誤認識誘発

- 画像敵対的サンプルの作成例（Yakura et al., 2020, AAAI）

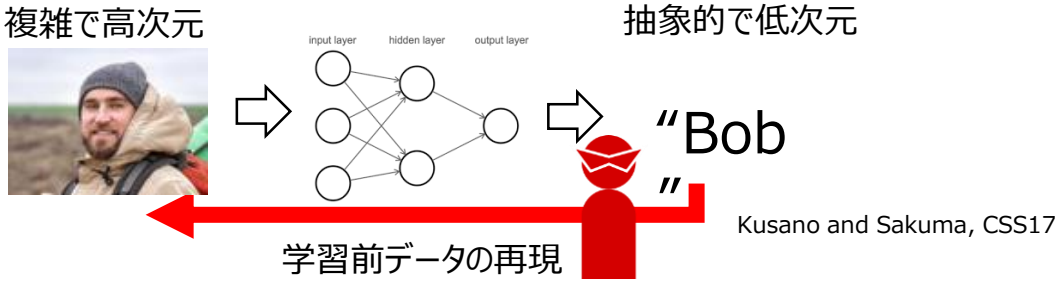

「止まれ」の標識に蝶々のステッカーが貼られてしまうだけで、AIは「速度制限」の標識と誤認識

- 音声敵対的サンプルの作成例（Yakura et al., 2019, IJCAI）


音楽にわずかなノイズを載せるだけで、スマートフォンの音声認識が「消防署への通報」と誤認識

## AIモデルの盗用

- 少ない情報量のアウトプットから多くの情報量を持つインプットデータの再現技術の発展（Kusano and Sakuma, 2017, CSS）




敵対的生成ネットワークの技術（既存のデータの特徴の学習によって、架空のデータ生成を可能にする）に加えて、適切な背景情報があれば、AIの逆問題を解き、学習前データの再現が可能

AIモデルの盗用と組み合わさることで、学習前の個人情報を含むデータの再現が可能となり、プライバシーへの甚大なリスクの可能性