「AI・データの安全・安心な利活用のための基盤技術・ルールの整備」検討タスクフォース決定

次期SIP課題候補「AI・データの安全・安心な利活用のための基盤技術・ルールの整備」Feasibility Study（FS）実施方針書ver1.0

2022年6月29日版

次期SIP課題候補「AI・データの安全・安心な利活用のための基盤技術・ルールの整備」について、検討タスクフォース（TF）を設置し、RFIの結果も参考にしつつ、社会実装に係る技術面、事業面などの観点でのインパクトや実現性の分析調査を行い、その結果を踏まえて取り組むべき研究開発テーマを抽出し、研究開発計画案を作成する。

対象とする課題候補	14　AI・データの安全・安心な利活用のための基盤技術・ルールの整備
課題候補のコンセプト	AIの利活用は急速に広がりつつあるが、その利活用においては、安全・安心が担保される必要性がある。その為には、プライバシーに配慮したデータの保護の促進と、敵対的サンプルなどのサイバー攻撃からAIの保護するという二つの異なる面からのアプローチが必要である。一方、AIの利活用拡大のためには、様々なステークホルダーのニーズに柔軟に対応できるデータ連携基盤を構築することが期待されている。これらの三つのコンセプトをプログラムの中核として行う。
目指すべき社会像と実現に当たっての社会課題	我が国が目指すSociety5.0では、様々なセンサーデバイスから収集される膨大なビッグデータを人間の能力を超えたAIが解析し、その結果がフィードバックされることで、新たな価値が産業や社会にもたらされる。さまざまなサービスやシステムでAI（人工知能）が活用されつつあり、これまで機械化が困難であった業務についても代替が可能となってきたことから、人手が減っている少子化への対策にもなりうることから、その社会的要求は今後さらに高まっていくことから、その要求に答えていく必要がある。 しかしながら、今後AIが高度に活用される社会を実現するのは、下記のようないくつかの課題を解決する必要がある。 現在のAIはそのほとんどが教師付き学習に基づいて予測・判断を行っていることから、多種・多様なデータがその学習には必要である。しかしながら、プライバシー、セキュリティ、倫理等の面から、自由に様々なデータにアクセスすることは実現できていない。特に日本では、中国やGAFA等に較べて、価値あるデータが各組織に分散してしまっている問題がある。そこで、プライバシーなどを保護しつつ汎用的にデータ解析ができる手法を確立する必要がある。 また、AIは学習によってその予測・判断を行うことから、異なる判断をもたらすような敵対的サンプルや汚染した学習データによるサイバー攻撃は問題となる。またAIの学習済みモデルを盗む攻撃や、出力からプライバシー情報を逆推定するなどもサイバー攻撃として考えられる。 一方、AIの利活用拡大には、高速性をもった大容量データ連携基盤の構築が必要であり、高速で動作する電子デバイスを用いたデータ連携基盤への要求が高まっている。
解決法とSIPで取り組むべきサブ課題の選定理由	上記の社会課題に対応するため、RFI結果の整理およびガバニングボードからのPD候補への期待などを踏まえ、まずは以下の三つを主なサブ課題として検討を行うことする。今後、各サブ課題において個別に検討すべき中核的な研究テーマを抽出し、技術実現性等調査を行うこととするとともに、サブ課題についての追加の検討も行う。 ①プライバシーなどを保護しつつデータ解析ができる秘密計算などの活用 [選定理由]　プライバシーを保護する観点と、データを広く共用化する汎用性は両立しづらいが、 データの収集・保存・活用すべてのライフライクルにおいてデータを一度も明かすことなく活用できる 秘密計算などの技術はこれらの問題を解決できる可能性を持つことから。 ②　サイバー攻撃からのAIの防護 [選定理由]　今後大きな脅威になるであろう各種サイバー攻撃からのAI（作成されたモデルへの攻撃も含む）防御の技術について取り組みを進める必要があることから。 ③　InP系電子デバイスによる高周波領域プラットフォームの構築 次世代半導体（ポストシリコン、高周波領域）として300GHz帯までの動作が現時点で期待出来るのはInP系電子デバイスのみに限られていることから。なお、通信用途だけでなくAIセンサー用途についても検討する。

課題候補の基礎的調査	目的	AI・データの安全・安心な利活用のために、我が国の強みを生かしつつ、上記のサブ課題の選定理由についての検証と課題の深堀をおこなうとともに、社会における重要性の評価を行う。
	方法	・技術開発動向調査 解決方法のうち技術開発に係るものについて、国際的な技術開発の動向や我が国のポジション等に係る情報について、国内外の論文・特許・標準化提案等の文献を通して調査し、国や組織の属性ごと技術分野別の強さ弱さに係る情報を入手すること。それらの結果とRFI 結果を踏まえて、有識者へのインタビューを9件以上実施し、取り組むべき研究開発テーマの検討に資する情報を提供すること。 なお、② サイバー攻撃からのAIの防護 については、RFIの提出がなかったことと、様々な攻撃があることに加え、技術的にも基礎検討段階であるため、広く意見を求め、またヒアリングを積極的に利用し、技術的な実現性を中心に確認を行うことも行う。 ・共通システムの構築やルール整備に関する調査 解決方法において技術開発に限らず、技術開発に伴う共通システムの構築やルールの整備等が必要なものについて、考慮すべき国内外の制度整備や関連施策の状況について文献調査と有識者へのインタビュー調査を3件以上実施し、その調査から現状と見通しに資する情報を抽出し提出すること。次期SIP において取り組むべき対応を検討TF で検討するに当たり、上記調査結果に基づいて、今後整備が必要となる可能性のある制度や規制等、関連所管省庁などの情報を提出すること。 ・国内外のプロジェクト調査 SIP が省庁連携のもとで推進されるプログラムかつ、国際連携を推進していることを踏まえ、上記の解決方法に関する国内外のプロジェクトの実施・検討状況を文献により調査し、一次情報または視覚化した二次情報（俯瞰的なマップ等）として、次期SIP との関係性を整理し、これにより省庁連携や国際連携のもとで取り組むことで課題解決に繋がる研究開発テーマの検討に資する情報を提供するとともに、ベンチマークとなるプロジェクトを抽出すること。 ・国内外の市場分析 解決方法に関する事業環境に関して、文献調査と有識者へのインタビュー調査を5件以上実施すること。具体的には、たとえば、想定される業界に係る国内外の市場規模と成長の見通し・バリューチェーンの各工程における主要企業の事業化状況など、日本企業の強み、弱み等、現状と見通しを検討TF で把握するに資する情報を提供すること。
サブ課題の中核的な研究開発テーマ候補の技術実現性等調査	目的	各サブ課題において個別に検討すべき中核的な研究テーマを抽出した上で、各テーマの技術実現性、事業性、社会的受容性に係る調査を行う。
	方法	3つのサブ課題について4テーマ程度を抽出し、各テーマ最大2千万円程度で技術実現性について調査を行う。また、事業性、社会的受容性についての調査も行う。 ・技術実現性調査：他技術等とのベンチマーク評価、ボトルネックとなる技術の調査、代替案の検討等を通じて技術的な実現性を調査 ② サイバー攻撃からのAIの防護 については、事業性・社会的受容性調査：ステークホルダーからのヒアリングを通じて需要と供給のポテンシャルを調査。

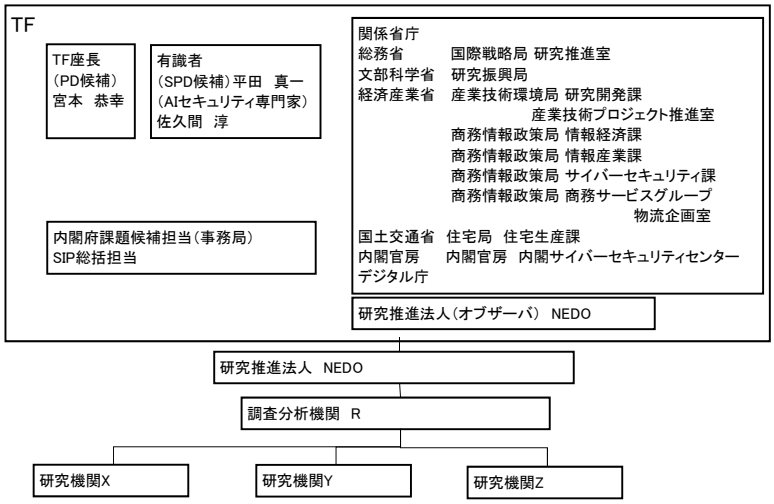
スケジュール

実施項目	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
TF活動		実施方針書Ver1.0決定▼ ※随時更新	基礎的調査方法▼		調査対象テーマ候補▼	選定	研究開発計画案作成▼	GB研究開発計画案審議▼		研究パブコメ・決定▼ 開発計画
FS調査公募手続（研究推進法人）		▼公募開始	▼公募締切	▼採択決定	▼契約締結					
基礎的調査（調査分析機関）							調査結果▼中間整理	フォローアップ作業		調査結果▼とりまとめ
テーマ候補の技術実現性等の調査（研究機関等）							調査結果▼中間整理	フォローアップ作業		調査結果▼とりまとめ
社会実装に向けた戦略検討（調査分析機関）							戦略素案▼作成	フォローアップ作業		調査結果▼とりまとめ
研究開発計画書素案作成（調査分析機関）							計画素案▼作成	フォローアップ作業		調査結果▼とりまとめ

予算（百万円）

項目	金額
・検討TF運営支援 ・基礎的調査 ・社会実装に向けた戦略検討 ・研究開発計画書素案作成	108
技術実現性等調査	72
一般管理費	20
合計	200

体制図



その他

＜本実施方針書に係る連絡先＞
内閣府　科学技術イノベーション推進事務局
社会システム基盤担当　福西
Tel：03-6257-1337