令和６年度補正予算 研究開発等計画

日本語版医療特化型LLMの社会実装に向けた安全性検証・実証

令和７年１月
経済産業省

● 実施する重点課題（特に該当するものには◎、そのほかで該当するものがあれば○（複数可）を記載）

SIPや各省庁制度による研究開発成果の社会実装・市場開拓の加速化	他の戦略分野等との技術の融合による研究開発	スタートアップによるイノベーションの創出・促進	産学官を挙げた人材の育成・確保	グローバルな視点での連携強化
◎	◎	◎		

● 関連するSIP課題（該当するものに○を記載）

持続可能なフードチェーン	ヘルスケア	包摂的コミュニティ	学び方・働き方	海洋安全保障	スマートエネルギー	サーキュラーエコノミー	防災ネットワーク	インフラマネジメント	モビリティプラットフォーム	人協調型ロボティクス	バーチャルエコノミー	先進的量子技術基盤	マテリアル事業化・育成エコ
	○												

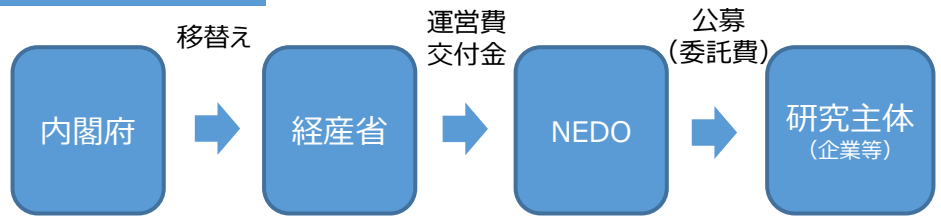
1．施策の概要

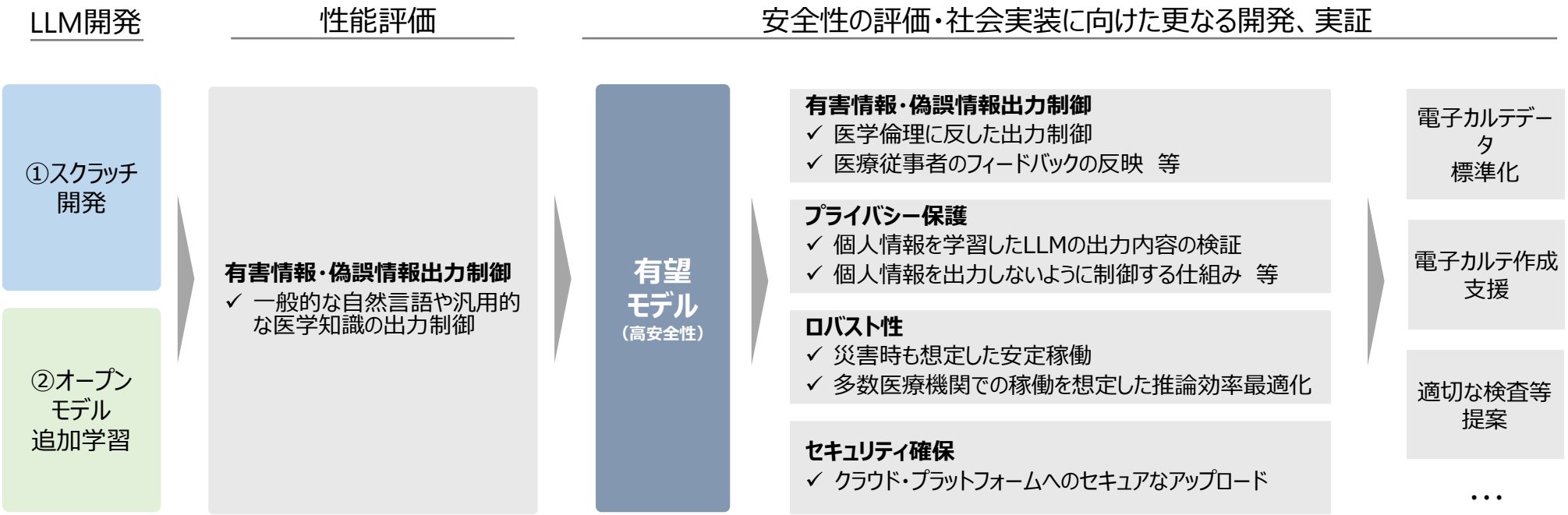
- 世界ではMeditronやMe-LLaMA等に代表されるような幅広い医療知識を持つ医療特化型LLMが台頭しており、**我が国としても医療現場での利活用を見越した性能を有する医療特化型LLMの開発**が求められる。
- **日本国内の医療特化型LLMの社会実装**に向け、医療現場で安心して利用してもらうAIサービス開発のためには、個人情報等のプライバシーの保護や有害情報・誤情報の出力制御等、医療用特化型LLMにおいて特に求められる機能を充足させ、**LLMの安全性を向上させることが重要**である。
- 医療分野での生産性向上に資するユースケースに**必要な情報から逆算し、リアルタイムで医師等に対して提案（電子カルテの作成支援、患者への適切な検査提案等）を行うことができるLLM**について、**スクラッチ開発やオープンモデルへの追加学習など、複数のモデルを構築しそれらの比較を行うことで、医療現場で安心して利用できるモデルを検証**する。
- 安全性が高いと見込まれるモデルについては、更なる安全性の検証や開発、実証を進め、**日本国内における医療現場でのAI利活用に繋げる**。

2．施策の対象・成果イメージ

- 医療現場では、多くの入力作業や事務作業が発生しており、医療従事者の労働環境の改善、人手不足の解消、医師が適格かつ素早く診断等を行える環境を整備するにあたり、安全で安心して利用できるAIを早期に実現することで、医療現場での人手不足等の諸問題を解決することが期待できる。

3．資金の流れ




LLM開発
性能評価
安全性の評価・社会実装に向けた更なる開発、実証
①スクラッチ開発
②オープンモデル追加学習
有害情報・偽誤情報出力制御
✓ 一般的な自然言語や汎用的な医学知識の出力制御
有望モデル
（高安全性）
有害情報・偽誤情報出力制御
✓ 医学倫理に反した出力制御
✓ 医療従事者のフィードバックの反映 等
プライバシー保護
✓ 個人情報を学習したLLMの出力内容の検証
✓ 個人情報を出力しないように制御する仕組み 等
ロバスト性
✓ 災害時も想定した安定稼働
✓ 多数医療機関での稼働を想定した推論効率最適化
セキュリティ確保
✓ クラウド・プラットフォームへのセキュアなアップロード
電子カルテデータ標準化
電子カルテ作成支援
適切な検査等提案
・・・

【事業を実施するにあたっての要件①】

１．医療特化型LLMの開発について

① 医療特化型LLM開発にあたっては、フルスクラッチでのモデル開発とオープンモデルへの追加学習や国内及び海外のオープンモデルへの追加学習等、複数のモデルを構築しそれらの比較を行うことで、LLMの基本的な性能としてどちらがより安全性が高いモデル（AIが不適切な挙動をしない、不適切な回答をしない、医療従事者を補助可能な適切な回答を出力する等）であるかを示すこと。

② ①の結果、より安全性が高いと見込まれるモデルについては、医療用特化型LLMとしての性能が発揮できるモデルとしての開発を進めること。

③ ②で開発した医療特化型LLMを医療従事者の業務補助ツールなどで実用化するにあたり、安全性を向上させるための研究開発、検証・実証を行うこと。 その際、１． 有害情報・誤情報の出力制御、２． プライバシー保護、３． セキュリティ確保、４． ロバスト性については必ず対応するものとし、その他、AIの安全性を向上させるために必要な研究開発等があれば提案してもらうこととする。

④ 上記②及び③の要件に基づき開発したモデルの社会実装の可能性を検証するため、医療現場でのユースケースを１つ以上想定した上でアプリケーション等を開発し、社会実装の可能性についての検証を行うこと。

２．実施体制について

⑤ 本事業では、開発した医療特化型LLMを社会実装に繋げることが主たる目的であることから、代表として申請を行う者は民間企業とすること。また、民間企業又は民間企業を中心とするコンソーシアムが中核となり、開発した医療特化型LLMの事業化やサービス化を行う事業構想を提案すること。

⑥ 医療特化型LLMの開発にあたっては、いわゆるスタートアップ企業の活躍にも期待しており、本事業の主たる開発を担う部分に中小企業基本法第２条の規程に該当する者を参画させること。

⑦ 事業全体を通じて医学的知見に基づく助言・監修が必須であり、医学的見地からのAIの安全性に関する助言・監修が行える者及び個人情報の取扱に関する助言・監修が行える者をそれぞれ複数名参画させること。

【事業を実施するにあたっての要件②】

３．AI学習用データの取扱について

⑧ 医療特化型LLMの開発にあたり、LLM学習用データを収集し、学習に適切な形式に変換するにあたっては、日本国内に法人格を有し、日本国内のみで変換作業を実施すること。

⑨ LLMの学習等においては、国内に設置されたデータセンターを継続的に利用出来る環境を整備すること。

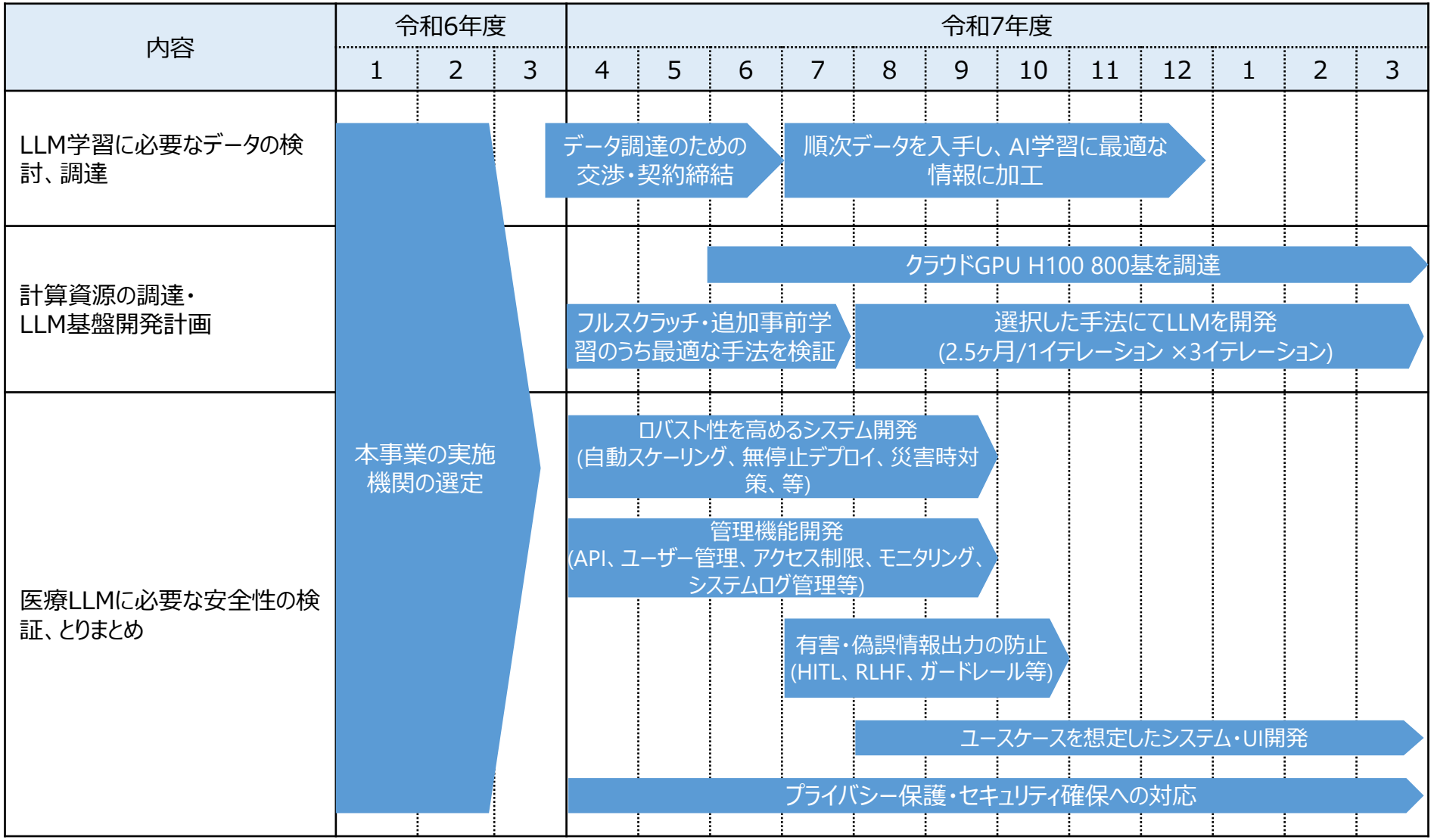
４．個人情報の取扱について

⑩ 医療特化型LLMを開発するにあたり、個人情報を含む医療情報を用いる場合には、「個人情報の保護に関する法律」、「次世代医療基盤法」及びこれらに関連する指針・ガイドラインを遵守して取り扱うこと。

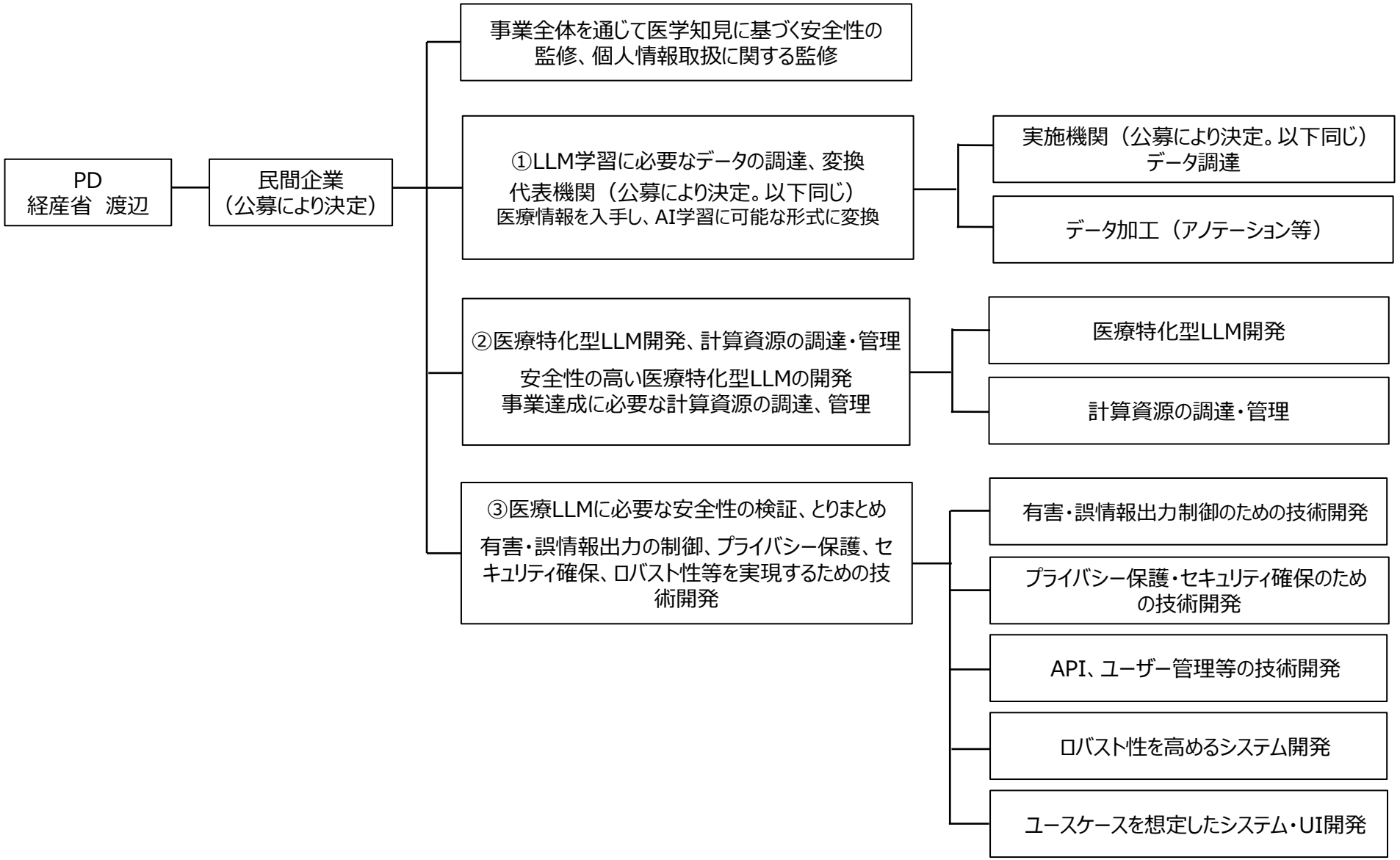
５．AIセーフティ・インスティテュート（AISI）との連携について

⑪ 国内のAI安全性に関する評価手法等の検討・とりまとめを行うAISIに対して本事業の取組状況や得られた成果について情報提供するとともに、AISI側から資料提供等の依頼があった場合には可能な限り対応すること。（企業秘密や個人情報に関するもの、対応にあたり多大な費用が発生するものは除く。）

5．取組スケジュール（想定）



６．実施体制（想定）


PD
経産省　渡辺
民間企業
（公募により決定）
事業全体を通じて医学知見に基づく安全性の監修、個人情報取扱に関する監修
①LLM学習に必要なデータの調達、変換
代表機関（公募により決定。以下同じ）
医療情報を入手し、AI学習に可能な形式に変換
実施機関（公募により決定。以下同じ）
データ調達
データ加工（アノテーション等）
②医療特化型LLM開発、計算資源の調達・管理
安全性の高い医療特化型LLMの開発
事業達成に必要な計算資源の調達、管理
医療特化型LLM開発
計算資源の調達・管理
③医療LLMに必要な安全性の検証、とりまとめ
有害・誤情報出力の制御、プライバシー保護、セキュリティ確保、ロバスト性等を実現するための技術開発
有害・誤情報出力制御のための技術開発
プライバシー保護・セキュリティ確保のための技術開発
API、ユーザー管理等の技術開発
ロバスト性を高めるシステム開発
ユースケースを想定したシステム・UI開発

７．実施内容・到達目標（KPI）

テーマ名	実施内容の概要 到達目標（KPI）
①　LLM学習に必要なデータの検討、調達	● LLM開発に必要な学習用データを入手し、AIが学習可能な最適な形式に変換。
②　計算資源の調達・LLM基盤開発計画	● LLM開発に必要な計算資源の調達。 ● フルスクラッチでのモデル開発とオープンモデルへの追加学習や国内及び海外のオープンモデルへの追加学習等、複数のモデルを構築しそれらの比較を行うことで、より安全性が高いLLMを選定。（TRL４：研究室レベルでの検証） ● 選定したLLMについて、医療特化型LLMとして研究開発、検証。（TRL４：研究室レベルでの検証）
③　医療LLMに必要な安全性の検証、とりまとめ	● 上記で選定したLLMについて、医療従事者の業務補助ツールなど、実用化可能なレベルに安全性を向上させるための研究開発、検証・実証を実施。 （有害・誤情報出力の制御、プライバシー保護、セキュリティ確保、ロバスト性　等） （TRL５：想定使用環境でのテスト） （BRL５：仮説検証）