科学技術振興機構報　第１７１２号

令　和　６　年　９　月　４　日

東京都千代田区四番町５番地３
科学技術振興機構（ＪＳＴ）
Tel：03-5214-8404（広報課）
URL https://www.jst.go.jp

経済安全保障重要技術育成プログラム（Ｋ　Ｐｒｏｇｒａｍ）における新規採択課題の決定について（令和５年度第３回募集　ＡＩセキュリティ）

ＪＳＴ（理事長　橋本 和仁）は、内閣府および文部科学省が定めた研究開発構想を受け、経済安全保障重要技術育成プログラム（Ｋ　Ｐｒｏｇｒａｍ）における新規採択研究開発課題を決定しました。

Ｋ　Ｐｒｏｇｒａｍでは、中長期的に日本が国際社会において確固たる地位を確保し続ける上で不可欠な要素となる先端的な重要技術を育成するため、国が定めた研究開発ビジョンや研究開発構想に基づき、研究開発を実施します。ＪＳＴでは研究開発構想（個別研究型）に関してはプログラム・オフィサー（ＰＯ）が、研究開発ビジョンの達成と研究開発構想の実現に向けて、研究開発課題の実施を指揮・監督します。実施に当たっては、研究開発課題提案の募集を行い、ＰＯが外部有識者らの協力を得ながら選考を行います。なお、公正で透明な評価を行う観点から、ＪＳＴの規定などに基づき、利益相反マネジメントを行います。

今回、以下の個別研究型の研究開発構想について、研究開発課題を採択しました（別紙１）。

「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」
公募枠：①一般研究開発
②データ基盤構築支援型研究開発
③知識・技術の体系化研究

今後、研究開発ビジョンの達成と研究開発構想の実現に向けて、より効果的・効率的な研究開発となるよう、採択された研究開発課題の研究代表者は、ＰＯの指揮の下で研究開発の詳細計画の作り込み（提案した研究開発計画の見直しおよび具体化など）を行った上で研究開発を開始します。

なお、「公募枠：①一般研究開発」に関しては、選考の結果を踏まえ、本日より研究開発課題の二次募集を開始します（募集締切：令和６年１１月５日（火）正午）。

詳細はＫ　Ｐｒｏｇｒａｍのウェブサイトをご覧ください。
ＵＲＬ：https://www.jst.go.jp/k-program/

＜添付資料＞

別紙１：採択研究開発課題一覧
参考１：経済安全保障重要技術育成プログラムの事前評価における選考の観点
参考２：経済安全保障重要技術育成プログラムにおける研究開発課題募集の概要

＜お問い合わせ先＞
科学技術振興機構 先端重要技術育成推進部
〒102-0073 東京都千代田区九段北４－１－７ 九段センタービル
小林 正（コバヤシ タダシ）
E-mail：k-program_koubo[at]jst.go.jp ※お問い合わせは電子メールでお願いします。

＜科学を支え、未来へつなぐ＞
例えば、世界的な気候変動、エネルギーや資源、感染症や食料の問題。私たちの行く手にはあまたの困難が立ちはだかり、乗り越えるための解が求められています。ＪＳＴは、これらの困難に「科学技術」で挑みます。新たな価値を生み出すための基礎研究やスタートアップの支援、研究戦略の立案、研究の基盤となる人材の育成や情報の発信、国際卓越研究大学を支援する大学ファンドの運用など。ＪＳＴは荒波を渡る船の羅針盤となって進むべき道を示し、多角的に科学技術を支えながら、安全で豊かな暮らしを未来へとつなぎます。
ＪＳＴは、科学技術・イノベーション政策推進の中核的な役割を担う国立研究開発法人です。

別紙１

採択研究開発課題一覧

研究開発構想（個別研究型）
「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」

公募枠：①一般研究開発

研究開発課題名	研究代表者（所属・役職）	研究開発概要
ＡＩハードウェアセキュリティ基盤技術の確立 （仮称）	本間 尚文（東北大学 電気通信研究所　教授）	本研究開発では、「ＡＩ　ｆｏｒ　Ｓｅｃｕｒｉｔｙ」時代におけるサイバーフィジカルシステムの耐タンパー性（物理的アクセスを伴う“物理攻撃”に耐える性質）の実装技術の確立を目指し、機械学習に基づく物理攻撃（ＡＩ物理攻撃）の技術を探求するとともに、同攻撃への対策技術の研究開発を推進します。特に、物理攻撃のフロントエンド（物理計測・前処理など）とバックエンド（データ解析など）にそれぞれ機械学習を利用する攻撃およびそれらを融合させた攻撃に関する知識・技術体系を整理し、その攻撃および防御理論を構築します。

公募枠：②データ基盤構築支援型研究開発

研究開発課題名	研究代表者（所属・役職）	研究開発概要
ＳＹＮＴＨＥＴＩＱ（シンセティック）Ｘ（エックス）：フェイク情報拡散の防御と予防を実現する研究基盤 （仮称）	越前 功（国立情報学研究所 情報社会相関研究系　教授）	本研究開発では、画像・映像、音声、テキストといった単一のモダリティ（データの種別）によるユニモーダルメディアに加えて、複数のモダリティで構成されたマルチモーダルメディアを対象に、フェイク情報拡散の防御技術と予防技術を確立します。さらに、リアル情報とフェイク情報からなる大規模データセットと多数の生成・防御・予防モデルで構成された、フェイク情報の生成とその防御・予防いう攻防の実践に適したフェイク情報研究基盤（ＳＹＮＴＨＥＴＩＱ Ｘ）を構築します。

大規模生成モデルを安全に運用するためのセキュリティ技術基盤 （仮称）	佐久間 淳（東京工業大学 情報理工学院　教授）	本研究開発は、大規模生成モデルの生成コンテンツのミスアライメント（人間の期待や倫理観から外れた挙動）を検出し、これを軽減・抑制するためのセキュリティ技術基盤の構築を目的としています。大規模生成モデルの利用においては、その生成コンテンツに有害情報・偽情報・差別的内容が含まれていたり、その生成コンテンツによって機密漏えい、プライバシー侵害、著作権侵害などが発生したりする可能性があり、このようなミスアライメントへの対策が不可欠です。一般の開発者が外部から入手した大規模生成モデルをそのまま利用したり、これを手元のデータで改変して利用したりする状況では、このようなミスアライメントのリスクを独力で評価することは簡単ではありません。本研究開発では、生成モデルのこのようなミスアライメントに関するリスクの評価を支援するための技術基盤を提供し、ミスアライメントの抑制につなげます。

公募枠：③知識・技術の体系化研究

研究開発課題名	研究代表者（所属・役職）	研究開発概要
安心安全なＡＩ利活用の為の知識・技術の体系化と知識集約環境構築 （仮称）	披田野 清良（株式会社ＫＤＤＩ総合研究所 セキュリティ部門　エキスパート）	本研究開発では、ＡＩセキュリティを社会に普及させることを目的とし、最新動向に配慮しながらＡＩセキュリティに関する知識・技術を網羅的に体系化します。また、体系化された知識に基づき論文や記事などの文献を効率的に収集・分類し、注意喚起や対策の普及啓発を効果的に行うための知識集約環境を構築します。本研究開発では、実際に構築した知識集約環境を利用してＡＩセキュリティに関する情報を発信しながら、その効果を実証します。

※研究開発課題名は調整により変更になることがあります。

参考１

経済安全保障重要技術育成プログラムの事前評価における選考の観点

１．研究開発ビジョンの達成および研究開発構想の実現に向けた達成目標の妥当性並びに多様な分野における研究成果活用の実現可能性

２．研究開発課題の達成目標に向けた実施内容の妥当性

- 研究開発項目・内容
- 実施体制
- 研究資金計画
- 安全管理措置の計画

※ 安全管理措置とは、研究開発に関する情報を適切に管理するための措置や、機微な情報に対する守秘義務履行のための必要な措置をいいます。

参考２

経済安全保障重要技術育成プログラムにおける
研究開発課題募集の概要

１．事業の趣旨

Ｋ Ｐｒｏｇｒａｍでは、中長期的に日本が国際社会において確固たる地位を確保し続ける上で不可欠な要素となる先端的な重要技術について、経済安全保障推進会議および統合イノベーション戦略推進会議が定めた研究開発ビジョンの実現に向け、内閣府および文部科学省が定めた研究開発構想に基づき、研究開発を実施します。
また、Ｋ Ｐｒｏｇｒａｍは経済安全保障推進法における特定重要技術の研究開発の促進およびその成果の適切な活用を目的とする事業に位置付けられています。

２．事業の特徴

研究開発構想には、重要技術の獲得を目指す比較的大規模な研究開発プロジェクトの研究開発構想（プロジェクト型）と、重要技術となり得る要素技術や研究開発プロジェクトの高度化に資する要素技術などの獲得を目指す個別研究の研究開発構想（個別研究型）があります。

研究開発構想（プロジェクト型）に関してはプログラム・ディレクター（ＰＤ）が、研究開発構想（個別研究型）に関してはプログラム・オフィサー（ＰＯ）が、研究開発ビジョンの達成および研究開発構想の実現に向けて、研究開発課題の実施を指揮・監督します。

また、関係府省との情報共有や意見交換の場などとして協議会が設置される予定です。

３．募集期間

令和５年１１月２２日（水）～令和６年２月８日（木）正午

４．ＪＳＴが研究開発課題を募集する研究開発構想

個別研究型

「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」

ＰＯ：松本 勉（産業技術総合研究所　フェロー）

※～令和６年３月　横浜国立大学 大学院環境情報研究院　教授

令和６年４月～　現職

以上