

「安全安心」分野のイノベーション政策強化推進にかかる
第 1 回、第 2 回のご意見のまとめ

1. 安全・安心に資する科学技術に関するシーズ・ニーズの把握と共有（「知る」）の仕組みの構築

- 政策立案機能とシンクタンク機能に関しては、国際的議論を日本の現状を踏まえて適切に行っている仕組みの検討が必要。特に技術専門家集団（目利き人材）の育成、確保が必要。
- 国立研究開発法人は、シーズ主導型で産学連携が弱い傾向にあるが、ニーズとのマッチングを促進するために、産学連携強化とシーズ情報を積極的に発信すべき。
- ニーズとシーズのマッチングには、目利き人材によるシンクタンク機能が必要であるが、安全・安心分野では、その機能が弱いため、強化が必要。また、シンクタンクの要件にも留意すべき。
- 政策実現のためには、国家戦略を実現するために重要なミッションを担う国立研究開発法人を省庁の横串連携で、活用することも重要。

2. 安全・安心に資する科学技術の研究開発の促進（「育てる」）の仕組みの構築

- 国際競争力の観点から、日本の強みを生かせる技術を特定して育てるためのプロジェクトが必要。
- 国は目指すべき方向性を示し、安定的にイノベーションエコシステムを回していくことが重要。
- 安全・安心に関わる研究では、個人情報保護法の枠組みの下で、個人情報を積極的に利用すべきである。その際は、社会に許容される、適切な利用目的を特定し、その達成に必要な範囲の中で利用していくことが重要。
- 民間が手を出せないようなリスクの高い技術開発は政府が投資すべきであり、安全・安心のような分野でムーンショット型研究開発事業を推進することが重要。
- たとえば防災ニーズを持っている側が、現状技術により何ができるかを検討し、それを実践する中で技術側に何が足りないかを同定し、それを次のフェーズの技術開発の要件につなげる、というサイクルが重要。
- 安全・安心分野の技術を民間が実証プロジェクトとして進めたり、サービスとして提供するビジネスを始めたりした場合は、政府又は自治体はそのプロジェクト等を継続して支援することが重要。その結果として、民間投資も進み本格的なビジネス化につながるループがまわることで継続性も現れる。
- 安全・安心技術は、緊急時のみの利用では、コスト効率が悪く、民間参入が困難。そのため、平常時の商業利用を考慮し、民間へのインセンティブを創出することが重要。
- 「安全・安心」分野での研究開発公募の際に、平常時は民間がその技術でどうビジネスをするかに関しても、あわせて提案してもらうことが一案ではないか。

3. 最先端の科学技術の国外への流出防止（「守る」）の仕組みの構築

- 「守る」は「育てる」と表裏一体であり、機微な技術が流出してしまうと大問題になるので、関係省庁が連携して取り組むべき。
- 国際的な技術覇権競争が起こる中、国際競争力の高い技術が海外流出のターゲットになるが、中小企業を含めた防止対策を省庁間で連携して対応することが重要。
- 「守る」取組として、中小企業を含めたサプライチェーン上の技術流出は深刻な問題となっており、対策について、議論が必要ではないか。
- 大学で生み出された特許の場合、大学と雇用関係に無い学生がした発明は職務発明に該当せず、大学に帰属させることが難しい場合があるため、海外等への技術流出の観点から注意が必要。
- 現状の特許制度は、公開が前提であるため技術流出の可能性が否定できない。特許情報を非公開にするなどの検討が必要ではないか。

4. 全般に係る仕組みの構築

- 自然災害やテロなどの緊急事態の対応に必要な技術は基本的に共通しており、すべてのハザードを対象に安全・安心という横串で包括的にイノベーションを議論することは意味がある。
- 個人情報保護法が、安全・安心の技術開発の支障になる場合がある。同法は、個人情報を特定の目的に従い使用するというものであり、その趣旨に沿って、安全・安心分野において活用することが重要。
- 安全・安心を確保するためには、サイバーセキュリティは重要な要素である。サイバー攻撃の脅威が高まる中、多種多様な攻撃への対策として、攻撃把握／攻撃予兆観測の高度化、対策の自動化、新技術への対応等が必要であり、加えて、攻撃を受けた後への対応も重要である。