案

重点的な研究領域について

資料4

我が国の強みとポテンシャルを踏まえ、知的価値及び社会的価値・経済的価値への寄与が大きいと考えられる研究領域は以下の通り。我が国のアカデミックな研究の強化に向けて、当面、この研究領域を念頭に、研究コミュニティの自主的な発展努力と相まって重点的な強化が図られることが望ましい。

安全・安心な社会基盤

デジタルインフラ（IoT、5G、クラウド等）セキュリティ

特にIoTセキュリティ研究領域は、欧米に比肩する強みのあるレベルと評価され、国内の観測網の整備等からポテンシャルとしてのさらなる強みもあると考えられる。IoTをはじめとするデジタルインフラを対象に重点的に強化を図るべきと考えられる。

サプライチェーンセキュリティ

米国が優位でそれに次ぐ欧州と同程度のレベルだが、国際的にもアカデミアでの研究発表はこれからと考えられる。あらゆる産業に関係し、当該リスクの検証技術など他国に容易に依存できない技術もあり得るため、重点的に強化を図るべきと考えられる。

データセキュリティ及びプライバシー保護*

欧米に比肩する強みのあるレベルと評価される。また、データは産業・社会活動の源泉であり、プライバシー保護は重要であるため、重点的に強化を図るべきと考えられる。

実装セキュリティ（ハードウェアセキュリティ含む）*

欧州が特に優位でそれに次ぐ米国や中国と同程度のレベルだが、実装段階のセキュリティに係る研究として、知識の蓄積があり、強みのある暗号研究にも関連しており、重点的に強化を図るべきと考えられる。

将来を見据えて取り組むべき分野

AIセキュリティ

米国が特に優位で欧州に次ぐレベルではあるが、トレンドは上昇傾向にある。AI戦略が策定され我が国においても社会実装が進むため、重点的に強化を図るべきと考えられる。

自動車セキュリティ

欧米が優位でそれに次ぐレベルだが、大きく差はついていない。自動車産業は世界的に強く、我が国として力を入れる実空間技術とサイバーとの融合領域（Society 5.0）であり、ポテンシャルとしての強みがあると考えられ、重点的に強化を図るべきと考えられる。

攻撃者優位を覆し先手を打つアプローチ

攻撃の視点から知見を得る（オフェンシブセキュリティ）研究**

攻撃者の視点に立って、リスクや脆弱性を洗い出し、対策する研究。防御中心のリアクティブな研究ではなく、技術から運用・体制に至るまで様々な角度から脆弱性を洗い出し対策するプロアクティブな研究は、進化する攻撃に対抗するためにも、重点的に振興を図るべきと考えられる。

実データの観測・分析に基づく研究**

攻撃状況や被害状況を含む実データの観測と分析をもとにしたデータドリブンアプローチの研究。サイバー空間の脅威状況を正しく理解し対策する研究に資するため、重点的に振興を図るべきと考えられる。

人的要素セキュリティ*

欧米が特に優位でそれに次ぐレベルだが、トレンドは上昇傾向にある。ユーザ認知の評価、ユーザインタフェース、トラスト、ソーシャルエンジニアリング対策など、日本においても人的要素の研究が行われてきたが、Society 5.0の実現とともに人的要素への配慮がさらに必要となると考えられるため、重点的に強化を図るべきと考えられる。

*は強み分析の整理における、基礎的要素に係る研究領域。無印は対象分野に係る研究領域。
**は強み分析において整理された個々の研究領域に当てはまらない横断的な手法・アプローチとしての研究分類であり、WGにおいて重点的な振興が重要と議論された研究。

※暗号研究分野の継続的な振興と国際的存在感の維持・向上等も極めて重要。また、科学研究費助成事業等による研究者の自由な発想に基づく研究は、発想・学理・シーズの源泉として極めて重要であり、引き続き推進されるべきものと考えられる。