重点的な研究領域について

資料3-3

（WG第3回会合資料2-3を基に作成）

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と重点的に強化を図るべきと考えられる理由（案）

対象分野に係る研究領域

（社会的／経済的価値への寄与の想定に基づき図示している）

社会的価値

経済的価値

サプライチェーンセキュリティ

（案）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まであまり見られず、これからと考えられる。サプライチェーンは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。

自動運転セキュリティ

（案）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）であるところ、ポテンシャルとしての我が国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。

AIセキュリティ

（案）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。

IoTセキュリティ

（案）欧米に比肩する強みのあるレベルと評価される。また、IoTデバイスの脆弱性発見等に関して国内の観測網が整備され、関連技術の軽量暗号や実装技術にも強みがあること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、重点的に強化を図るべきと考えられる。

基礎的要素に係る研究領域

データセキュリティ及びプライバシー保護

（案）欧米に比肩する強みのあるレベルと評価される。また、データは産業活動の源泉であり、データ利活用の促進にはデータの保存・交換・処理の安全性を確保する必要があるため、重点的に強化を図るべきと考えられる。

人的要素セキュリティ

（案）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。人的要素は日本の社会や産業の特性である品質や細やかさの基盤であり、その面からのフィードバックが得られる可能性があるため、ポテンシャルとしての我が国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。

実装セキュリティ（ハードウェアセキュリティ・暗号実装含む）

（案）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、過去の経緯から半導体やハードウェアの研究者が多く、知識の蓄積があり、強みのある暗号研究にも関連しているため、重点的に強化を図るべきと考えられる。

（横断的な手法として重点的に振興を図るべき研究）

攻撃研究（仮称）

（案）攻撃者の視点に立って、未知の脅威を発見し攻撃に悪用される前に対策する研究である。今後は水際対策・事後対策から脱却し、事前対策を行うことで根本からの問題解決を目指す必要があるため、重点的に振興を図るべきと考えられる。

検知（観測）に基づく研究（仮称）

（案）ネットワーク・システム・サービスの運用時のデータを活用するデータドリブンアプローチでの研究である。対策手法の評価検証だけでなく、実態調査に基づいて最新の攻撃情報を把握し、新たな対策技術の研究に活用できるため、重点的に振興を図るべきと考えられる。