令和3年(2021年)3月
サイバーセキュリティ戦略本部 研究開発戦略専門調査会
研究・産学官連携戦略ＷＧ

資料１－１

「サイバーセキュリティ研究・産学官連携戦略ＷＧ最終報告」（概要）

～研究開発の国際競争力を躍進させる産学官エコシステムの構築～

第1章 はじめに

若く伸びている研究分野

・国際的なトップカンファレンスへの論文投稿が2000年に比し約４倍以上。
・我が国でも、2010年代に主な研究集会への参加者数が２倍以上に成長。
（サイバー空間の拡大と実空間との融合を背景に、国際的に存在感が高い暗号研究コミュニティの継続的でオープンな発展努力と様々な分野からの研究人口の流入。）

コラボレーションが非常に活発

・国際的に、国際共著論文、産学官連携論文が増えている。中国の存在感が年々増大。
・デジタル活用とセキュリティ対策の一体性が深くなり、セキュリティに係るアカデミックな研究が、富や活力を生み出す源泉の両輪の一つと理解されている。

▷ **今は産学官にわたるエコシステムを構築する重要期 ／ 我が国におけるデジタル化と同時並行で進める必要**

第2章 我が国の研究コミュニティの状況を踏まえた推進方策

▷ **エコシステム駆動に向けた循環の構築**

2.1 研究分野の国際動向と特徴

・欧米では博士課程学生がフルタイムで給料を支払われ、貴重な研究戦力に。
・本分野では、情報系分野と同様、柔軟で優秀な「人材」が大きく研究を進展させ得る。
（コンピュータサイエンスを基盤とし、プログラミングや試行錯誤が多く必要となる点が特徴。）

2.2 人に投資すべき

・博士課程では、本分野でも、専門分野の知識・方法論の修得が基本だが、一定の実社会経験が重要。
（インターンや産学共同研究など。セキュリティの現場とデジタルの現場の両面で機会の創出・拡大が望ましい。）
・リサーチアシスタント（RA）経費の有効活用と上限柔軟化が重要。
（研究プロジェクトや産学共同研究費にて、RA経費で優秀な博士課程学生を迎えて大きく研究を進める。上限の柔軟な設定・運用が非常に重要。そのための人材公募も。）
・RA経費の活用で、社会人を含む博士課程進学の様々な形態を可能に。
（さらに、次世代にとってのキャリアパスの魅力向上と博士人材のキャリア形成支援に取り組む。研究室を越えてコンソーシアム的に取り組むことが効果的かつ重要。）

2.3 産学官連携の可能性

・連携相手は潜在的に多い。欧米では相応規模のデータや研究費の授受を伴う共同研究。我が国でも、研究費を人に投入する産学共同研究が今後検討されるべき。
（通信事業者、ITベンダー企業、セキュリティベンダー企業に加え、インターネット企業やDXを進める様々な企業等を連携相手とし、経営的かつ潜在的なニーズに応え得る研究構想が重要。）
・アカデミア発ベンチャーも、一つの産学官連携の形態として注目される。

2.4 研究コミュニティ全体の発展

・ファンディングの機会と研究費の活用が重要。
（国やファンディング機関の企画立案に当たり、研究コミュニティの状況や動向が良く踏まえられることで、活発な提案申請がなされやすい。本分野の研究コミュニティの活力や様々な研究構想を結びつけていくことが重要。）
・科学的基礎の構築、プロシーディング論文を含む柔軟な研究実績の評価
（他分野や実社会との協働において科学的手法が提供できる価値の中心的な概念を言語化。情報・セキュリティ系分野では重要なプロシーディング論文も、ファンディング申請等で研究実績に含まれる旨を明確化すべき。）
・研究者や研究機関の国際交流・国際展開を活発に行うことが重要。
（海外武者修行を含めた国際的に活躍する若手研究者の育成や国際共同研究の振興等に取り組む。）

第3章 我が国の強み・ポテンシャルと重点的な強化に向けて

3.1 我が国の強みとポテンシャル

・IoTセキュリティやデータセキュリティ・プライバシー保護など米欧に比肩する研究領域がある。
・Society 5.0の実空間・サイバーの融合領域に係る研究領域、暗号研究の強みを活かした研究領域等には、ポテンシャルとして強みがある。

3.2 重点的な研究領域

・上記を踏まえ、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等の理由で、重点的な強化が図られることが望ましい研究領域は以下の通り。
（※研究者の自由な発想に基づく研究も、発想・学理・シーズの源泉として引き続き重要。）

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 データセキュリティ・プライバシー保護	サプライチェーンセキュリティ 実装セキュリティ（ハードウェアセキュリティ含）	
将来を見据えて取り組むべき分野	AIセキュリティ	自動車セキュリティ	
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	実データの観測・分析に基づく研究	人的要素セキュリティ

産学官の様々なステークホルダーから期待を持ってもらうため、具体例を提示。
（※今後適時リバイス・ピボットされ得る。他にも新たな構想が生まれてくることを奨励・歓迎。）

3.3 研究構想の具体例

◆DFFT（信頼ある分散型データ活用）研究
A　社会的・経済的データ共有・分析基盤
B　攻撃観測データ共有・分析基盤
C　共通技術の深化・高度化
DFFT: 信頼性のある自由なデータ流通

◆人工知能セキュリティ研究
A　機械学習のCIA確立
B　機械学習のセキュリティ技術への応用
CIA: 情報セキュリティの重要3要素

3.4 産学共同研究構想の具体例

◆サービスのセキュリティ強度評価手法
大学 × インターネット企業／ユーザ企業

◆ソフトウェア堅牢化手法の有効性研究
大学 × ソフトウェア開発企業

◆端末利用者のリスク低減研究
大学 × セキュリティベンダー企業

第4章 むすびと今後の展望

・我が国のサイバーセキュリティ研究開発の国際競争力を躍進させるため、産学官エコシステムの構築を中心ビジョンとして、課題解決を実現するための方策を多角的に議論、整理。
・本WGの取組をきっかけとして、今後も議論・意見交換が持続的になされていくことを期待。