

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。
(RA経費で優秀な博士課程学生を研究戦力として迎えて大きく研究を進める観点。情報・セキュリティ系分野では上限を柔軟に設定・運用できることが非常に重要。)
- ・研究プロジェクトや産学共同研究費において、RA経費を柔軟に設定し、優秀な人材を迎える形態が本分野には必要。欧米のように、そのための人材公募も。
(これにより社会人を含む博士課程進学の様々な形態を可能に。なお学生の教育や学位取得の厳格さも重要。)

2.3 産学官連携の可能性

- ・サイバー空間の拡大・融合に伴い、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。)

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よく踏まえらるることで、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生み出される研究構想を結びつけていくことが重要。)
- ・科学的基礎に係る概念、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概念を言語化。情報・セキュリティ系分野ではプロシーディング論文も重要であり、ファンディング申請等において研究実績に含まれる旨を明確化すべき。)

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欧米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される等の理由で、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とおり。
(※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	サプライチェーンセキュリティ	
	データセキュリティ・プライバシー保護	実装 (ハードウェアセキュリティ含) セキュリティ	
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ense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

産官学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

- ◆ サービスの安全性評価手法確立
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 今後に向けて

- ・今後、研究コミュニティとの意見交換や研究開発戦略専門調査会での議論等を踏まえ、最終報告に向けた本WGの議論の重点等を検討。
- ・構想の具体例は、本報告が刺激となり、様々な場で検討されるきっかけとなることを期待。