資料３

産学官連携に係る議論の整理素案

【中間報告より抜粋】　※赤字は追記箇所

２．３　産学官連携の可能性

サイバーセキュリティ分野における研究は、サイバー空間において運営されるシステム、プロダクト、サービス等のセキュリティ現象・事象を対象とするため、研究コミュニティにとって、企業等の連携相手は潜在的に多い。

これまでも産学連携は行われているが、他分野と同様、年間数百万円といった少額のものが多く、企業側から見れば大学・研究機関とのコネクション形成、リクルート、自社の研究者のレベルアップといった目的が結果的に多くなっているものと考えられる。

一方、海外では産学の人材流動によるものや、プロジェクトや論文成果となるような相応規模のデータや研究費の授受を伴う共同研究が実施されていると考えられ、アカデミア発ベンチャー企業がインパクトあるエグジットに到る事例も見られる[15]。これには、欧米の大学で見られる、柔軟で優秀な博士課程人材を迎え入れ、研究を大きく進める手法もとられていると考えられる。

２．３．１　研究費を人に投入する相応規模の産学共同研究

我が国のセキュリティ分野の産学官連携においても、柔軟で優秀な人材が大きく研究を進展させ得るため、研究費を人に投入する観点の産学共同研究が今後検討されるべきと考える。その場合、結果として、少額ではなく相応規模の産学共同研究になると想定される。

デジタル化やDXの進展が求められる我が国において、今後、デジタル技術を活用したビジネスとそのセキュリティ需要は拡大することはあっても縮小することはなく、連携相手は、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となる。連携を想定する先の企業の以下のような経営的かつ潜在的なニーズに応え得る研究構想が重要になると考えられる。

（連携想定先企業の経営的かつ潜在的なニーズ例）

・企業の重要な収益を担っている又は支えているコアなシステムが、中長期的に、ユーザやニーズ等の増大や、サイバー攻撃の高度化・巧妙化等があっても、盤石性を保てるか。
・新たにシステムを構築する際、科学的基礎に基づくセキュリティ検討を同時並行的に付加したり、新規事業に向けて、革新的な知識・アイディアの創出を狙ったりする必要はないか。
・企業が保有するデータについて、セキュリティの学理や最新の研究に基づく分析を行い、有益な示唆が得られないか。

２．３．２　ベンチャー起業

研究成果や研究構想を実社会で実現する際、ベンチャー起業も重要な選択肢となる。海外では、アカデミアで活躍する教授が、大学の研究成果をネットワークセキュリティ製品にしてベンチャーを創業し、製品によって収集が可能なデータを大学で分析し、アカデミアでも成果を出すといった、データドリブンアプローチのベンチャー・産学連携の事例が見られ、我が国でも参考になると考えられる。

また、近年、大学ではアントレプレナーシップ教育が行われるようになっているが、情報系の分野と同様、一人や少人数チームのアイディアや試行錯誤が世界を変え得るため、学生の志向等に応じて教員が雰囲気作りなどの後押しを検討することも重要と考えられる。

15 添付資料参照。

追加素案

２．３．３　共同研究強化のためのガイドライン

産学共同研究を進める上で、知的財産権の適切な取扱いや契約の締結が重要になるが、一般的に、従前の例に沿った硬直的な交渉が行われたりするといった指摘がある。

これに関して、関係省庁により、産学官連携による共同研究強化のためのガイドライン[16]が策定されており、研究成果の活用を見据えた柔軟な契約交渉、事業化までを想定した契約締結等につき処方箋が提示されている。また、11 類型のモデル契約書をまとめたツール[17]が提示され、大学・公的研究機関や企業の知的貢献、経済的貢献に応じた知的財産権の取扱い等のモデルが示されている。

我が国のセキュリティ分野においても、本ガイドラインを活用し、柔軟かつ効率的な産学の交渉が促進され、産学共同研究が促進されることが期待される。

16 「産学官連携による共同研究強化のためのガイドライン」（2016 年 11 月、文部科学省・経済産業省）及び「追補版」（2020 年 6 月、文部科学省・経済産業省）。

17 「産学官連携による共同研究強化のためガイドライン　追補版」（2020 年 6 月、文部科学省・経済産業省）における「さくらツール」（日本版ランバート・ツールキット）。