サイバーセキュリティ研究・産学官連携戦略ワーキンググループ中間報告案~~（ドラフト）~~

～~~（副タイトル）~~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～

令和２年１０月２２~~１２~~日
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・産学官連携戦略ワーキンググループ

目次

第１章　はじめに

１．１　経緯及び背景

サイバーセキュリティに係る分野（以下、セキュリティ分野ともいう）におけるアカデミックな研究が国際的に急成長している。トップカンファレンスでの論文投稿は、2000年に比し約4倍以上となる2000本超が毎回投稿される規模となっており、採択を巡って切磋琢磨が行われている[1]。

さらに、アカデミックな研究にあって、プレーヤーは、コンピュータサイエンスを主導してきた米国主要大学に止まらない。Microsoft、Google といったメガプレーヤー、Samsung、Huawei といった新興企業や欧州等の大学等が参画しており、2010年代に入って、これらプレーヤーの国際共著論文や産学共同研究などコラボレーションが非常に活発になっている。

世界的にデジタル化・IT利用・インターネット接続が大きく経済社会を牽引し、種々の産業がインターネット上に移行しており、デジタル技術の活用とサイバーセキュリティ対策の一体性や両輪性はより深くなっている。前者に係るものと同様、サイバーセキュリティに係る現象・事象を根源的に理解し深化させる営為、すなわちアカデミックな研究が、そのまま富や活力を生み出す源泉の両輪の一つであると理解され、産学連携を含むコラボレーションが活発化しているものと考えられる。

我が国においても同様の萌芽が見られる。我が国の大学等のアカデミックな研究活動は論文数の停滞など概して困難な状況も指摘されているが、本分野においては、国内の主な研究集会~~カンファレンス~~の参加者数が、2010年代に入って、およそ2倍以上の800人を超える規模に成長していることが特筆される[2]。また、国際的なカンファレンスに採択される論文成果も増加傾向にある。

これには、長らくそして現在も、国際的に一定の高い存在感を示している我が国の暗号研究の研究コミュニティの存在があり、その継続的でオープンな発展努力と、魅力を増す研究分野全体への様々な分野からの研究人口の流入が主要因として挙げられよう。これによって、純理論系の暗号研究に留まらず、ここ10年～20年で、サイバー空間そのものやサイバー空間が拡大している様々な実社会を対象として、新たな研究が数多くなされるようになってきた。若く伸びている研究分野と言える。

コロナ禍で明らかになったように、我が国のデジタル化は焦眉の急であり、サイバー空間の拡大と実空間との融合が政策的にも大きく進められようとしている中で、今後も本分

1　~~研究コミュニティで~~国際的に著名でアカデミックな研究発表の場として主要と考えられている研究集会（カンファレンス）。サイバーセキュリティに係る分野では、IEEE Security & Privacy、ACM CCS、USENIX Security、NDSSの4つがそれに当たるほか、そのうち暗号研究分野では、Crypto、Eurocryptが著名。これらのカンファレンスでは、論文が投稿された後、ピアレビューで査読され採択されたもののみが論文（プロシーディング論文）として研究発表される。

2　情報処理学会「コンピュータセキュリティシンポジウム（CSS）」では、2010年代初頭の300人台から、2019年には2倍以上の800人台に増加。また、電子情報通信学会「暗号と情報セキュリティシンポジウム（SCIS）」でも着実に増加し2019年に800人台に増加。それぞれ年1回、研究集会が開催される。

野への社会的要請は高くなることはあっても低くなることはない。国際的にも、科学的基礎に基づくセキュリティ対策がより重要性を増すと考えられるところ、アカデミックな研究の発展への期待は高い。

同様に、昨年5月の~~「~~サイバーセキュリティ研究・技術開発取組方針[3]~~」（研究開発戦略専門調査会）~~が指摘した政策課題である~~我が国~~~~産学官連携のコミュニティ形成についても、他国に目を向ければ、アカデミアのベンチャー起業をはじめ、活発に産学官連携の事例が生まれているところ、我が国においても、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い。産学官連携の機会とポテンシャルは小さくないと考えられる。

このように、社会的要請の高まりが継続的に見込まれ、また、産学官連携を含め、より魅力的な研究分野へと発展するポテンシャルが存在する研究分野において、その研究と産学官連携の振興に向けた推進方策を検討することが重要との認識の下、研究開発戦略専門調査会の下に本ワーキンググループ（以下、WG）が7月に設置された。

今こそ、そして、今後数年間こそが、我が国の研究コミュニティの活力を更なる発展ポテンシャルと結びつけ、産学官にわたるエコシステムを構築するための重要な時期であると考える[4]。それは我が国のデジタル化と同時並行で進まねばならない。その認識の下、審議を行った結果を中間報告としてまとめた。

１．２　研究開発戦略や研究・技術開発取組方針との関係

我が国の~~「~~サイバーセキュリティ研究開発戦略~~」~~[5]は、研究開発を検討・推進するに当たっての基本的な考え方や方法論を提示し、「今後（中略）具体的なサイバーセキュリティの研究分野やテーマについて検討を行うなど本戦略を具体化」することとされているが、本WGの検討は、アカデミックな研究を中心とした、その具体化の一環となる。

また、~~昨年5月の「~~サイバーセキュリティ研究・技術開発取組方針~~」~~[6]にて、政府の取組の具体化及び強化の方向性が示されているが[6]、本WGの検討は、方向性の1つとして示された「産学官連携の研究・技術開発のコミュニティ形成」の深堀りであり、ここで謳

---

[3] 2019年5月 研究開発戦略専門調査会決定。

[4] エコシステムは、サイバーセキュリティ研究・技術開発取組方針では、「産学官の関係者が連携し、相互の取組の情報共有や研究活動における連携を図る」ものとされている。本報告では、アカデミックな研究を中心として、産学官が連携し、相互に良い影響を及ぼし合いながら、研究や事業等が複層的に生み出され、進化していく姿を、一種の生態系にたとえたものをいう。

[5] 2017年7月 サイバーセキュリティ戦略本部決定。我が国の将来のサイバーセキュリティの研究開発を検討・推進するためのビジョンとして策定され、第2章にて基本的な考え方や方法論、第3章にて中長期的な検討の切り口を提示。それらは現時点でも変わらないものと認識される。それらに基づく現在の研究開発の推進については、現「サイバーセキュリティ戦略」（2018年7月 閣議決定）や~~「~~サイバーセキュリティ研究・技術開発取組方針~~」（2019年5月 研究開発戦略専門調査会決定）~~に反映・記載されている。

[6] ~~2019年5月 研究開発戦略専門調査会決定。~~今後の取組強化の方向性として5つが示され、①サプライチェーンリスクへ対応するためのオールジャパンの技術検証体制の整備、②国内産業の育成・発展に向けた支援策の推進、③攻撃把握・分析・共有基盤の強化、④暗号等の基礎研究の促進、⑤産学官連携の研究・技術開発のコミュニティ形成となっている。

われた「産学官の関係者が連携し、相互の取組の情報共有や研究活動における連携を図るためのエコシステムの構築に向け、基礎となる体制を整備する」ことを目指した検討である。

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

我が国における本分野のアカデミックな研究と産学官連携が、相互に良い影響を与えながら発展するために重要と考えられる推進方策を以下に示す。検討に当たっては、研究開発戦略専門調査会で示された様々な課題[7]について、それらの連関に鑑みつつ、アカデミックな研究を取り巻く産学官のエコシステムが回るために重要と考えられる課題を中心に検討を行った。

２．１　研究分野の国際動向と特徴

サイバーセキュリティに係る分野のトップカンファレンスでは、毎年論文投稿が増加し、国境を越えたあるいは産学官の垣根を越えたコラボレーションが活発化している[8]。

その中心として、米国の大学等が長らく非常に高い存在感を示しているが、ドイツ・フランス・スイスといった欧州の大学等がそれに次ぐ存在感を示している。また、カナダ、シンガポール、中国、韓国、イスラエルの大学等の存在感が認められ、特に中国の存在感が年々増大している。我が国大学・研究機関の存在感は限定的であるが、近年、採択論文は増加傾向にある。なお、サイバーセキュリティに係る分野のうち、暗号研究分野では、トップカンファレンスで我が国の一定の高い存在感が認められる。

このアカデミックな研究活動を支える基盤として、米国では、様々なファンディング機関が存在し、特定分野の応用研究を中心に担う DARPA や IARPA がセキュリティ関連の複数の研究プログラムを運営しているほか、全米科学財団（NSF）が、セキュリティ分野の基礎研究を幅広く支援する公募プログラムに年間 50 億円強の予算を継続的に充てていることが特筆される。欧州においても、EU の Horizon 2020 から同程度の予算により継続的に公募プログラムが運営されている[9]。

さらに、人的な面では、セキュリティ分野において欧米では博士課程学生がフルタイムで給料を支払われて、研究グループにとっての貴重な研究戦力になっていることが指摘されているが[10]、これが欧米の旺盛な研究活動の基盤のもう一つの側面となっているものと考えられる。

サイバーセキュリティ研究では、サイバー空間における「システム」（コンピュータ、

7　研究開発戦略専門調査会において本 WG が設置された第 14 回会合の資料 2 参照。事務局がプレリミナリーな意見交換を 50 名程度の有識者・研究者と実施した際に挙げられた本分野の振興に向けた様々な課題を指す。

8　4 つのトップカンファレンス（IEEE Security & Privacy、ACM CCS、USENIX Security、NDSS）では、国際共著論文の割合は 43%であり、産学官連携論文の割合は 20%となっている（2019 年の採択論文について NISC 調べ）。添付資料参照。

9　WG 第 3 回会合資料 1-3 及び第 4 回会合参考資料 2 より。

10　研究開発戦略専門調査会で示された様々な課題の 1 つ（第 14 回会合資料 2 の課題 1 参照）。

ネットワーク、関連機器や、それら動作のアルゴリズムやプロトコル、あるいは様々な者が提供・使用するプロダクトやサービスなどの単体あるいは複合）に係る現象・事象を対象とすることが多い。そして、システムの観測や模擬システムの構築、それらの解析や対策研究において、コンピュータサイエンスを基盤とし、研究行為としてコンピュータを用いたプログラミングやその試行錯誤を中心としたものが多く必要となる点が特徴として挙げられる。

すなわち、柔軟な発想ができ、進展の早い最新の計算機・プログラミング環境を駆使できる、優秀な「人材」が大きく研究を進展させ得る分野と言える。そして、欧米では、この点を最大限に活かした研究推進を図っているものと考えられる。いわば、学問体系に基づく PI[11]の指導の下で、一人あるいは少人数チームの学生・若者のアイディアと試行錯誤が世界を変え得るという観点である。この点は情報系の研究分野でも同様と考えられる。また、システムに係る研究は、時には研究室を越えて様々な強みを持つ「人材」が連携し組織的に研究を進めることで進展することもある。

研究が構想され、資金が獲得され、その資金を「人」に投入して、研究を進める。研究の中で育った「人」が、さらに学問を発展させ、研究拠点や研究グループを作り、産学官連携を進め、次の研究を構想する。

欧米の動向はもとより、研究分野の特徴を踏まえれば、こういった循環により研究推進を図ることが非常に重要である。本分野の研究コミュニティは、若いコミュニティがゆえ、コミュニティ全体としての発展をこれから模索できる段階にある。上記で挙げられた様々な課題では、博士課程学生の役割が海外と異なる、大型産学連携やベンチャー起業が少ない、ファンディングが活用できていないと言った課題が挙げられているが、この循環構築に向け取り組むことが、課題解決となり、エコシステムを駆動する鍵になるのではないか。本 WG はそう考える。

なお、国やファンディング機関のファンディングには、主に、i）研究者の自由な発想に基づく研究を支援するもの（科学研究費助成事業等）、ii）国の方針に基づき研究領域等が定められその中で研究者が提案するもの、iii）府省が進める研究開発プロジェクトがあるが、本報告では、ii）を念頭に、研究コミュニティの発展可能性をさらに高めるにはどうすればよいかといった観点から検討を行っている。

２．２　人に投資すべき

本分野では、柔軟で優秀な人材が大きく研究を進展させ得るため、研究費を人に投資する、すなわち、研究費を柔軟で優秀な博士課程学生やポスドクに大胆に投入して迎え入れ、研究を進展させる観点が重要である。

11　Principal Investigator（主任研究者）。研究グループを主宰する研究者で、大学においては教授等となる。

２．２．１　博士課程学生

欧米大学では、博士課程学生が研究プロジェクトの研究戦力になっている。一方で学生の教育や学位取得の厳格さも重要である。

一般的に、博士課程では、近年、アカデミックな研究職のみならず、企業をはじめとする社会の多様な場で活躍する人材の輩出が期待されてきた。すなわち、アカデミアでは知的価値、社会的価値や経済的価値の基礎となる研究成果を生み出し、産業界ではイノベーション創出の中核を担い、あるいは、産学協働の場では産学にまたがる知識の全体を俯瞰し異分野を融合するリーダーとなる者を育成することが期待されている。

サイバーセキュリティ分野においても、他分野と同様、専門分野の知識や方法論を強みとして身につけることが基本となるが、上記の人材像を念頭に、一定の種々の実社会経験を通じ、経験の幅に加え俯瞰力と独創力を養うことが重要である。インターンシップ、企業との共同研究、社会人ドクターとの深いディスカッションの実施等が考えられ、大学と企業が一体となって育成を行うことも考えられる。

その際、サイバーセキュリティ対策につき CSIRT[12]等の現場経験のない学生にはそれに触れる機会を創出・拡大し、デジタル技術の活用や DX ~~や IT 活用~~につき企業の現場経験のない学生にはそれに触れる機会を創出・拡大するなど、サイバーセキュリティとデジタル技術の ~~DX・IT~~ 活用の両面から機会の創出・拡大を図ることが望ましい。研究室や大学内の研究組織で産学連携や学内連携を模索することがまず考えられるが、大学を越えた研究室・研究組織の広域連携により、そのような機会を創出・拡大することも考えられる。

２．２．２　リサーチアシスタント（RA）経費の有効活用と上限柔軟化

博士課程への進学を検討する者にとって、経済的支援が十分であるかどうかは重要な判断要素である。情報・セキュリティ系の分野では、研究者が獲得する研究費で研究を進める際、他分野と同様に研究設備等のハードに係る経費に研究費の多くの部分を充てることが重要になる研究もあるものの、ソフト、とりわけ博士課程学生を、RA 経費を用いて研究戦力として迎えることで大きく進む研究があり、研究の内容に応じて後者を柔軟に選択できることが合理的であり、かつ、研究分野全体の発展に資すると考えられる。

また、情報・セキュリティ系の分野では、AI 等の進展もあり民間企業の給与水準が一般的に高くなっており、優秀な人材を博士課程に迎えるには、現状多く見られる程度の支給額では、現実的な経済的インセンティブとして働かないと考えられる。

このため、これら分野において、RA 経費の上限を柔軟に設定・運用できることが非常に重要である。

12　Computer Security Incident Response Team の略。コンピュータセキュリティに係るインシデントに対処するための組織の総称（一般社団法人日本シーサート協議会）。

なお、内閣府の総合科学技術・イノベーション会議においても、「海外と同様に、博士を目指す学生は『研究者』としても扱われるべきという発想の転換が必要。博士後期課程学生の研究活動に対する適正な対価の支払いを当たり前にするとともに、生活面での心配をすることなく研究に打ち込めるよう、国を挙げて支援を実施・加速化」するとされており[13]、この方向性を推進すべきである。

２．２．３　社会人を含む博士課程進学の様々な形態

これまで社会人博士課程に多く見られた進学例として、企業に在籍したまま企業から給与を受け大学院に進学し、学位を取得し、元の企業に復職するという形態がある。そして、今後、本分野で研究者が獲得した研究費を「人」に投入することが進めば、新たな形態となり、上記に加えた様々な選択肢が社会人並びに修士課程からの進学者を含め可能となる。

それは、国・ファンディング機関から獲得する研究プロジェクトや、企業から獲得する産学共同研究費において、提案申請や研究計画立案の際にRA経費の上限を柔軟に設定し、その研究期間内で、RA経費の対象となる優秀な博士後期課程学生を迎え入れ、標準修業年限を終えるという形態である。優秀な人材を迎え入れるために、欧米大学のように研究プロジェクトに係る人材公募を広く行うことも考えられ、博士課程への入学選抜も行われる。

これにより、研究面では、柔軟で優秀な人材を得て研究を大きく進めることができ、人材にとっては、フルタイムでの進学検討のインセンティブとなるような経済的支援が得られ、最先端の研究プロジェクトや産学共同研究への参画で実践的な素養・能力を培って実績を得られるとともに、学位取得に繋げられ、キャリアップの可能性が拓けるというメリットがある[14]。

これまで我が国では見られなかった形態であるが、本分野には必要である。可能な研究グループから試みて研究推進と人材育成の幅を広げることにより、次世代にとって魅力的なキャリアパスを形成していくことが重要と考えられる。なお、推進に当たっては、研究プロジェクトや産学連携に従事させることと、博士号取得に至る専門性や独創力等の養成をどう両立させるかといった学生の教育の方法論につき研究コミュニティとして議論を深めることが重要と考えられる。

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

13　総合科学技術・イノベーション会議第50回（2020年7月16日）「研究力強化・若手研究者支援総合パッケージ」の進捗状況／進捗状況と今後の方向性より。

14　添付資料参照。なお、産学共同研究費を提供する企業にとっては、研究面が進展する他に、育った人材が自社の次のプロジェクト等で即戦力やリーダーとなり得るというメリットも考えられる。

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~~投入し~~、研究を大きく進める手法もとられていると考えられる。

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~~トレンド~~に基づく分析を行い、有益な示唆が得られないか。

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

15 添付資料参照。

る。

２．４　研究コミュニティ全体の発展

本分野は、若く伸びている分野として、研究コミュニティ全体としての発展をこれから模索できる良い段階にあると考えられる。

研究が構想され、資金が獲得され、その資金を「人」に投入して、研究を進める。研究の中で育った「人」が、さらに学問を発展させ、研究拠点や研究グループを作り、産学官連携を進め、次の研究を構想する。こういった循環を構築したい。

２．４．１　ファンディングの活用

２．１で述べた ii) 国の方針に基づき研究領域等が定められその中で研究者が提案するファンディングは、国やファンディング機関が行う企画立案に当たり、研究コミュニティの状況や動向をよく踏まえたものとなれば、活発な提案申請がなされやすい。また、企画立案に当たって研究者を交えたワークショップ等が開催される場合もある。

こういったファンディングの機会と研究費を研究コミュニティ全体として活用し、研究構想を実現し、研究拠点や研究グループを形成していくことが重要である。そして、ファンディングの企画立案に、研究コミュニティの活力とそこから生み出される研究構想を結びつけていくことが重要と考えられる。研究コミュニティの発展に向けて、様々な研究構想がなされ、研究提案がなされることが望ましい。

なお、その中で、本 WG としては、今回、研究構想が持つべき基本的な特性として、以下を挙げて検討を行った。

(研究構想が持つべき基本的な特性として考えられるもの)

・国際通用性

例えば、国際的なカンファレンスで発表する、世界のトップレベルと交流する、世界と渡り合える研究グループが育つもの。

・人材育成

例えば、次の世代を担う博士号取得者が育つもの。

・次につながる

例えば、産業界や投資家に出口戦略が見え、大きな関心が示され、共同研究やベンチャー起業を複層的に生み出すもの。重点的な研究開発プロジェクト(国プロ)に発展し得るような研究成果を複層的に生み出すもの。

研究コミュニティの発展において、研究拠点の形成は、象徴的な意味合いを持つ重要な取組となる。我が国の国際的な顔となり、次世代にアピールし、「人」が集まって流動し、研究構想や産学共同研究を複層的に生むベースとなる。今後さらに検討を深めるべきであるが、その形態としては、サイバー空間を対象としている研究分野であるため、その特徴を活かして、PI を結ぶネットワーク型の拠点形成と一定の PI が集まる物

理的な拠点形成のハイブリッド型の形成などが考えられよう。また、大学だけでなく公的研究機関が役割を持って関与する形態も構想され得ると考えられる。

２．４．２　科学的基礎に係る概念~~【P】~~

本分野は、今世紀に入ってサイバー空間がさらに拡大する中で急速に発展している若い分野であり、いわゆる統一的な理論や定番的な教科書といったものが現時点で存在するわけではないが、科学的基礎に基づくセキュリティ対策の実社会における需要は広がる一方と考えられる。

現在の内外のセキュリティ対策において、科学的に確立され十分に理解された解決策は、社会の様々な分野・領域に偏在するのみであり、分野・領域や文脈に特有のものが多いと考えられる。また、数学的及び実証的な妥当性が十分に検証されておらず、有効性や効率性が考慮されていない場合もあると考えられる。このような対症療法的で発見的（ヒューリスティック）な手法は、進化する技術や変化する脅威や攻撃に対して、信頼できるシステムを維持するためには不十分・不完全で、重要な脆弱性を見落とし得ると言える。

このため、引き続き、科学的基礎を構築していくことが重要である。

また、研究コミュニティにとって、研究の対象として、あるいは、産学官連携のコラボレーションの相手として、様々な応用的な他分野・実社会との接点が拡大することが想定され、これら他分野・実社会から、本分野のアカデミックな研究と協働することで何が期待できるか、科学的手法が提供できる価値の中心的な概念は何か、理解してもらう必要性は高まろう。

このため、これまで培われ、共有され、発展してきた科学的基礎に係る概念を一旦言語化する作業を以下の通り試みた。これについては新たな知見や学問の発展等とともに見直されるものである。また、この科学的基礎自体について、その確立・構築・発展を目指して取り組む理論的な研究はさらに重要になってくると考えられる[16]。

（サイバーセキュリティ研究の科学的基礎）

1. システムを評価する際において、脅威を定量的に測定する方法、安全性を測定可能な形で保証する方法、防御機構と攻撃者を効果的・効率的に評価する方法
2. 安全なシステムを設計する際において、システムが満たすべきセキュリティの特性と効果を証明可能あるいは定量的に検証可能とする方法
3. 破壊的イノベーションなど新たに生まれるテクノロジーや急激に変化する攻撃者によって生じ得る脅威を予見する、あるいは未然に防ぐ方法
4. 社会で用いられるシステムにおけるセキュリティ・安全性・プライバシーに関す

16　米国連邦サイバーセキュリティ研究開発戦略計画においても科学的基礎の構築の重要性が謳われている。WG 第 4 回会合参考資料 2 及び参考資料 3 参照。この科学的な基礎に係る概念は、この資料を参考として加筆修正したものである。

る、個人・組織・社会の要求、期待および行動原理を理解するための理論とモデル
以上の方法は、いずれも科学的な手法に基づき記述され、客観的に再現性がある形で実行されるべきである。

２．４．３　プロシーディング論文を含む柔軟な研究実績の評価

研究者の研究実績として評価されるものとして、論文誌（ジャーナル）での論文成果（ジャーナル論文）と研究集会（カンファレンス）での論文成果（プロシーディング論文）が挙げられるが、プロシーディング論文が評価されにくい場合があるとの指摘がある[17]。

プロシーディング論文は、査読・フィードバック・掲載が迅速であることから、研究の進展が速い情報・セキュリティ系の研究分野において馴染みが深く、中でも査読付きで評価の高いものは、国際通用性のある研究実績とされることが多い。実際、海外ではトップ級のカンファレンスでの論文成果が評価され、近年は日本からも重要なカンファレンスに採択されるプロシーディング論文が増えてきている。

一方、プロシーディング論文が重要であることは、他分野の研究コミュニティからは必ずしも理解されにくい。研究費の申請書においても、研究実績はジャーナル論文であることが前提であるかのように誤解し得る記入例が示されている事例が存在する。本来は、研究実績をどのように評価するのかについてはそれぞれの研究コミュニティにおいて判断されるべきものではあるが、特に情報・セキュリティ系の分野では、査読付きで研究コミュニティ内でも評価の高いプロシーディング論文が研究業績として適切に認められることが、研究者にとって、さらには当該分野の発展にとって、極めて重要である。また、その評価のあり方が分野の内外に伝わるよう、積極的に発信する必要がある。

このため、情報・セキュリティ系の研究分野では、ファンディング機関等における研究費申請書において、プロシーディング論文も研究実績に含まれる旨を明確化すべきである[18]。

17　研究開発戦略専門調査会で示された様々な課題の１つ（第 14 回会合資料 2 の課題 2 参照）。

18　具体的には、国およびファンディング機関における研究費申請の申請書・記入要領において、「情報・セキュリティ研究分野ではプロシーディング論文も実績として含む」といった明確な注意書きを記載する。

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

我が国の本分野の研究競争力を高め、国際的な存在感を増し、産学官のプレーヤーとのコラボレーション等を通じてサイバーセキュティに係る知見の増大と技術革新を生んでいくためには、アカデミックな研究の重点的な強化が欠かせない。

それには、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とともに、研究コミュニティの発展可能性を高め、様々な研究構想や研究提案がなされ、「人」が育ち、研究拠点や研究グループが作られていくような「研究領域」を見出し、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重要である。

３．１　我が国の強みとポテンシャル

上記「研究領域」を見出すため、まずは我が国の現在の国際的な立ち位置に基づく強みとポテンシャルを踏まえることが重要である。

このため、我が国の過去 5 年の研究集会で設けられた研究セッションであって、純理論系の暗号研究分野を除く、実践的なサイバーセキュリティの研究分野のものを一定の領域のまとまり毎に網羅的に整理を行った。なお、我が国の暗号研究分野は、トップカンファレンスで国際的に一定の高い存在感を示している。

この研究領域の整理に基づき、本 WG でアカデミックな研究レベルの国際比較の分析作業を行い、現状の我が国の強みとして添付資料の成果を得た。14 の分析対象の研究領域のうち、ほとんどの領域で米国あるいは米欧が強いが、IoT セキュリティ研究領域や、データセキュリティ及びプライバシー保護研究領域など、米欧に比肩する領域があり、国際的な受賞など我が国の顕著な活動・成果が見えている領域や我が国が上昇傾向にある領域が存在する。

一方、我が国の研究コミュニティの特性や、社会や産業等の特性を考慮して、ポテンシャルとしての我が国の強みには、以下が挙げられると考えられる。

（ポテンシャルとしての我が国の強み）

- IoT や自動車など実空間技術とサイバーとの融合領域（Society 5.0）は、我が国として強みかつ力を入れるため、そのセキュリティを研究する、IoT セキュリティ研究領域や自動車セキュリティ研究領域といったサイバーフィジカルシステム（CPS）に係るセキュリティは、日本の強みとなるポテンシャルがある。
- 我が国の暗号研究は国際的にみても強みを有しており、暗号研究の強みを生かしたセキュリティ評価・リスク評価研究領域（システムのセキュリティ設計やセキュリティ分析に係るもの）や、データセキュリティ及びプライバシー保護研究領域（個人データの利活用を促進するための加工技術に係るデータ保護（匿名化技術）・秘密計算（マルチパーティ計算など））などは、日本の強みとなるポテンシャルがある。
- セキュリティ製品やシステムの品質や実運用への配慮にも現れる細やかさは、我が国の社会や産業等の特性の一つと考えられ、その基盤を支え、フィードバックが得られ

る可能性がある人的要素セキュリティ研究領域は、日本の強みとなるポテンシャルがある。

３．２　重点的な研究領域~~【P】~~

上記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~~」~~は以下の通りである。その検討の際、現状では強みが必ずしも認められなくても、例えばサイバー犯罪等の脅威に対するセキュリティといった、価値への寄与が大きいため強化を図るべきものや、他国に依存することが望ましくないため強化を図るべきものも見出された。

我が国のアカデミックな研究の強化に向けて、当面、これら~~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と考える。

もちろん、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、実践的なサイバーセキュリティの研究分野の研究との相互に良い影響を与えながらの発展も極めて重要である。

なお、２．１で述べた i) 研究者の自由な発想に基づく研究を支援するファンディング（科学研究費助成事業等）による研究は、発想・学理・シーズの源泉として極めて重要であり、これら~~の「~~研究領域~~」~~に限らず、個々の研究者の自由な発想に基づき、引き続き推進されるべきものである。

（重点的な研究領域）

強み分析を行った研究領域のうち、強みがありポテンシャルや価値への寄与が大きい研究領域、現状では強みが必ずしも認められないもののポテンシャルや価値への寄与が大きい研究領域、強み分析の個々の研究領域に当てはまらないものの横断的な手法・アプローチとして重点的な振興が重要と考えられる研究を以下の通り挙げた。また、それらを３つの観点からグループに分け整理している。

［安全・安心な社会基盤］

経済社会の安全・安心な社会基盤を支える研究領域

・デジタルインフラ（IoT、5G、クラウド等）セキュリティに係る研究領域

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研究領域

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研究領域*[19]

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）研究領域*

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］

将来の経済社会を見据えて重点的に強化を図るべき研究領域

・AI セキュリティ研究領域

米国が特に優位で欧州に次ぐレベルではあるが、活動・成果の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研究領域

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］

サイバーセキュリティ全般に攻撃者には防御側と比べて非対称な優位性があるが、攻撃や被害が認識されてから防御を考える対策だけでなく、先手を打った対策につなげていくために重要と考えられる研究や研究領域

・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**[20]

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

19 *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。なお、デジタルインフラセキュリティは、強み分析を行った研究領域ではないが、IoT を含む、経済社会を支える幅広いデジタルインフラを対象としつつ、その中で知的価値及び社会的・経済的価値への寄与の大きいものを重点的に振興することは重要との観点から WG の議論において追加されたもの。

20 **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。

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研究領域*

欧米が特に優位でそれに次ぐレベルだが、活動・成果の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。

さらに、科学的基礎の確立・構築・発展に取り組む理論的な研究が今後益々重要性を増すと考えられる。

３．３　取り組むべき研究構想の具体例

取り組むべき研究構想の具体例として以下が挙げられる。

（取り組むべき研究構想の具体例）~~（P）~~

・信頼ある分散型データの活用を実現するセキュリティ基盤技術（DFFT 関連技術）

プライバシー等を保護しつつ分散型データを活用するためのセキュリティに関する基盤技術の確立を目指す研究構想（別添資料参照）

・人工知能セキュリティ

人工知能（機械学習）が浸透する社会において機械学習とセキュリティに関する基盤技術の確立を目指す研究構想（別添資料参照）~~（P）~~

３．４　取り組むべき産学共同研究構想の具体例

取り組むべき産学共同研究構想の具体例として以下が挙げられる。

（取り組むべき産学共同研究構想の具体例）~~（P）~~

・サービスの安全性に関する評価手法の確立

大学等の連携相手として、インターネット企業や DX を進めるユーザ企業を念頭においた共同研究構想（別添資料参照）

・商用ソフトウェアの脆弱性対策と堅牢化手法の有効性研究

大学等の連携相手として、ソフトウェア開発企業を念頭においた共同研究構

想（別添資料参照）

・端末側での利用者のセキュリティリスク低減に向けた分析・把握に係る研究

大学等の連携相手として、セキュリティベンダー企業を念頭においた共同研究構想（別添資料参照）~~（P）~~

上記の研究構想の具体例は、今後検討され得る様々な研究構想を含め、産学官の様々なステークホルダーから、我が国のアカデミックな研究の発展に期待をもってもらうための具体例として提示したものである。状況に応じ適時リバイス・ピボットされ得るものであり、あくまで現時点における例示として示すものである。

いずれにせよ、こうした具体例に限らず、他の新しい研究構想が研究コミュニティから生まれてくることを奨励・歓迎したい。

第４章　今後に向けて~~【P】~~

本 WG は、本年 7 月から 6 回にわたり集中的に議論し、中間報告をとりまとめた。研究開発戦略専門調査会で示された様々な課題について、エコシステム構築に重要と考えられるものを中心として、全般的に一定程度触れることはできたと考える[21]。

今後、研究コミュニティとの意見交換や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することとしたい。

第 2 章で示した人への投資は、次世代にとっての将来のキャリアパスの魅力増につながるべきものである。博士課程に関して今回新たに示した推進方策は、その後のキャリアップの可能性を高めるものと信じるが、今後、具体事例が創出されることを期待しつつ、最終報告に向けて議論をさらに深めたい。

次世代という観点で言えば、~~SECCON や~~ SecHack365、enPiT、高専における人材育成、セキュリティ・キャンプ、SECCON 等の人材育成プログラムは、優秀な技術者を育て裾野を広げているが、こういった中からも、アカデミックな研究に興味を持ち、進学・従事・関与する者が益々増えることで我が国の産学官のエコシステムがさらに重層的なものになるといった視点も重要と考えられる。

なお、アカデミックな研究レベルの国際比較（強み分析）に係る作業は、この形の先行取組がなく、WG として初めての作業であった。最終報告に向け、必要に応じブラッシュアップしていきたい。

また、研究構想や産学共同研究構想の具体例の提示については、時間的制約があったことも事実であるが、本 WG 中間報告が刺激となり、様々な場で研究構想や産学共同研究構想が検討されるきっかけとなることを期待したい。

21　研究開発戦略専門調査会で示された様々な課題（WG 第 1 回会合資料 1-8）のうち、1、2、6、7、9、10 については本文で取り上げ、3 や 4 に関しては科学的基礎の概念で、5 は研究コミュニティ全体の発展で、8 や 11 に関しては第 3 章で一部触れた。11 に関連し、研究コミュニティが研究活動の幅を広げるに応じ、研究倫理について様々な場で議論が深められることが重要と考えられる。

審議経過

第１回　令和２年７月 29 日
（１）ワーキンググループについて
（２）研究・産学官連携の推進方策に係る議論について
（３）分野・領域に係る議論について

第２回　令和２年８月６日
（１）研究・産学官連携の推進方策に係る議論について
（２）分野・領域に係る議論について

第３回　令和２年８月 28 日
（１）研究・産学官連携の推進方策に係る議論について
（２）分野・領域に係る議論について

第４回　令和２年９月 10 日
（１）研究・産学官連携の具体に係る議論について
（２）中間報告に向けて
（３）その他

第５回　令和２年９月 29 日
（１）研究・産学官連携の具体に係る議論について
（２）中間報告に向けて
（３）その他

第６回　令和２年 10 月 12 日
（１）中間報告案について
（２）その他

研究開発戦略専門調査会
研究・産学官連携戦略ワーキンググループ　委員名簿

主査	森　達哉	早稲田大学理工学術院　教授　（専門調査会委員）
	秋山　満昭	NTT セキュアプラットフォーム研究所　上席特別研究員
	荒木　粧子	株式会社ソリトンシステムズ　IT セキュリティ事業部／Soliton-CSIRT エバンジェリスト
	須賀　祐治	株式会社インターネットイニシアティブ　シニアエンジニア
	高橋　健太	株式会社日立製作所　主管研究員
	永山　翔太	株式会社メルカリ　R4D（研究開発部門）　シニアリサーチャー
	本間　尚文	東北大学電気通信研究所　教授
	山内　利宏	岡山大学大学院自然科学研究科　准教授
	山田　明	株式会社 KDDI 総合研究所　研究マネージャー
	吉岡　克成	横浜国立大学大学院環境情報研究院・先端科学高等研究院　准教授

（主査以下五十音順、敬称略）