資料１

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最終報告案

～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３年３月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留まらない。Microsoft、Googleといったメガプレーヤー、Samsung、Huaweiといった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

1　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の四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。

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、2019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]が指摘した政策課題である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2020年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さらなる発展ポテンシャルと結び付け、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最終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、サイバーセキュリティ研究・技術開発取組方針にて、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、方向性の一つとして示された「産学官連携の研究・技術開発のコミュニティ形成」の深掘りであり、ここで謳われた「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。

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、一種の生態系に例えたものをいう。

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・技術開発取組方針に反映・記載されている。

6　今後の取組強化の方向性として五つが示され、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。

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、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

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　四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一つ（第 14 回会合資料 2 の課題 1 参照）。

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、進展の速い最新の計算機・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良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。

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

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。

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付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 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 経費をはじめとする経済的支援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 経費をはじめとする経済的支援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。

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。

---

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）。

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。

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、元の企業で勤続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、大学側だけでなく企業側も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、学位取得につなげられ、キャリアアップの可能性が拓けるというメリットがある[14]。このように、産学官のエコシステムが積極的に活用されていくことが望ましい。

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。

２．２．４　次世代にとってのキャリアパスの魅力向上とキャリア形成支援

セキュリティ分野の博士課程に関して今回新たに示した推進方策は、進学者や社会人、さらには次世代にとって、博士課程修了後のキャリアアップの可能性を高めるものと考える。

中でも、２．２．１で示した、博士課程における産学で協働した実社会経験や現場経験の機会の創出・拡大は、博士課程学生がその後のキャリアを具体にイメージするためにも、学の側が企業等とのネットワークを構築・維持し、博士人材へのキャリア形成支援に活かすためにも重要と考えられる。

これについては、本分野における博士人材キャリア形成支援策の一環として、一つの

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、研究面が進展するほかに、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。

研究室・研究組織に留まらず、産業界を含む研究コミュニティで、広域連携その他の方法により、有志等によりコンソーシアム的に取り組むことが効果的かつ重要と言え、具体の取組が望まれる。こういった取組の中で、博士人材の横のつながりの醸成、産学による人材育成及び官も含む人材流動化の機会を創出・拡大すること等も期待される。

さらに、次世代という観点で言えば、SecHack365、enPiT、高等専門学校における情報セキュリティ人材育成事業、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。

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至る事例も見られる[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、または支えているコアなシステムが、中長期的

15　添付資料参照。

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。

こういったニーズに応え得る研究構想が大学・研究機関側から提案されることが重要であり、大学等において構築されている組織的な産学官連携体制や企画・マネジメント機能を活用して企業側に積極的な提案とコミュニケーションをすることも考えられる。また、企業側のニーズに対し、大学等のシーズ情報が見える化され研究者や研究テーマをマッチングする取組やコーディネーター等の活用も有益であると考えられ、様々な試みがなされることが期待される。

こうした産学共同研究が様々に模索され進展する中で、人文社会科学を含む科学的手法が生み出す価値やそれに対する企業等からの期待が高まっていくことが望まれる。例えば、企業のシステム等に関わるリスクの見える化・定量化や、サイバーセキュリティ対策の有効性や効率性等の科学的手法に基づく検証を行う産学共同研究が模索され進展すれば、産学双方に大きなメリットを生み出す可能性がある。企業の経営層にとって、採るべきセキュリティ対策の合理性への納得が深まり、セキュリティ対策への投資が推進されるような研究構想とその進展が望まれる[16]。

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、セキュリティ分野の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。

アカデミア発ベンチャーは、様々な分野で我が国においても重要なプレ―ヤーとなっており、先進的なベンチャー創出支援に取り組む大学等や、こうした大学等を中心とするベンチャーキャピタル・金融機関等の連携も見られる。セキュリティ分野においても、大学・研究機関と企業との連携を検討するに当たって、その間にあるアカデミア発ベンチャーという柔軟で機動的な組織形態のメリットを活かすことで、大学・研究機関がベンチャーを通じて企業のニーズにより応えていくことも可能と考えられ[17]、一つの

16 科学的手法が生み出す価値等に関する科学的基礎の構築について２．４．２参照。また、取り組むべき産学共同研究構想の具体例として３．４及び添付資料の一例目を参照。

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）p.7 の記述参照。

産学官連携の形態として注目される。

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。

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[18]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[19]が引用され、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。

また、本ガイドラインには、知的財産権以外にも、研究成果として創出された知への価値付け、人材を循環・流動化させるための兼業・クロスアポイントメント制度の活用等の産学官連携における組織的連携をスムーズに進めるための処方箋が提示されている。さらに、大学等への処方箋だけでなく、大学等と産業界の両者を対等なパートナーとして、産業界向けの記載も新たに体系化されている。

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。

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良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

18　「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）。

19　2016 年度文部科学省委託調査「大学における知的財産マネジメント事例に学ぶ共同研究成果の取扱の在り方に関する調査研究」における「さくらツール」（日本版ランバート・ツールキット）。

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付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　科学的基礎の構築

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[20]。

（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、セキュリティ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. セキュア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・セーフティ・プライバシーに関する、個人・組織・社会の要求、期待及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[21]。

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

20　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。

21　研究開発戦略専門調査会で示された様々な課題の一つ（第 14 回会合資料 2 の課題 2 参照）。

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[22]。

２．４．４ 国際交流・国際展開

研究コミュニティ全体が発展していく上で、世界の産学官ネットワークの一角に位置付けられ、存在感を示して発展につなげる観点、また、世界の知を取り込み、国際競争力を強化する観点から、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非常に重要である。

このため、海外での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に取り組む。科学研究費助成事業を含むファンディング機関等の国際関係の支援制度の活用が期待されるほか、各研究機関における留学制度等の独自の取組や公的な留学制度の活用も奨励される。中でも、我が国と相手国のファンディング機関で国際共同研究の共同公募（ジョイントコール）や共同支援が連携して行われる制度[23]は、両国連携のワークショップ等が開催され交流の機会が拡大し得るほか、相手国の共同研究者に当該国側から研究費が措置されるため、相手のインセンティブやモチベーションが高い中で共同研究が推進できる。積極的な活用が期待されるとともに、このようなファンディングの企画立案にも、研究コミュニティの活力と研究構想を結び付けていくことが重要である。

さらに、現状では、我が国研究コミュニティの国際的なカンファレンスのプログラム委員や実行委員等の運営側への就任は少ないが、論文採択を含めた存在感の向上、意義あるカンファレンス等の我が国への招致、国際的な研究動向等に相通じた我が国研究コミュニティの発展と世界的な貢献にとって重要である。今後、これらの委員を増やす努

22 具体的には、国及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。

23 例えば、総務省の戦略的情報通信研究開発推進事業（SCOPE）国際標準獲得型や科学技術振興機構（JST）の戦略的国際共同研究プログラム（SICORP）。

力を行うとともに、研究コミュニティ全体として努力を適切に評価しこれらの委員を支援していくことが重要である[24]。

２．４．５ 最先端の研究活動のための取組

加えて、研究コミュニティが研究活動の幅を広げるに応じ、前例のない先進的なサイバーセキュリティ研究を推進するためには、社会に受容されるような倫理的配慮が必要となる[25]。例えば情報処理学会コンピュータセキュリティシンポジウムにおける取組では、これを支援する取組の一つとして、サイバーセキュリティ研究における倫理的配慮のためのチェックリストを作成し、論文投稿時の研究倫理相談窓口を設け、典型的な倫理的配慮を論文著者に啓発している。なお、先進的研究が社会に理解され受容されることは重要ではあるが、倫理的配慮の名の下に先進的研究をストップさせるような圧力になることは避けるべきである。先進的研究を「萎縮させない」ためにも、各組織の経営層を含め、様々な議論や活動を通じて理解が醸成され、適切な倫理的配慮を実施する土壌が広がることが望まれる。

また、2020 年からの新型コロナウイルス感染症の影響により、研究活動においても物理イベントの開催等に制約が生じているが、一方で、オンラインによる地理的な制約を超えたコミュニケーションが一般的かつ容易になった面があり、研究コミュニティ内の交流はもとより、産学官連携や国際交流など研究コミュニティの発展につながる活動において一定の可能性を広げていると言える。VR/AR 等のデジタル技術の活用や物理イベントとのハイブリッド開催など、オンライン活用のさらなる工夫により、最先端の研究活動を模索することも望まれる。

---

24 プログラム委員等の運営側への就任を継続的に有益なものとするため、委員個人に蓄積されるノウハウやネットワーク等を研究コミュニティで共有する取組も望まれる。

25 研究者のみならず研究を指導・リードする立場の者の意識も重要となる。

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見ても強みを有しており、暗号研究の強みを活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

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、それらを三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、都市 OS 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*[26]

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**[27]

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

---

26 *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。

27 **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基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）

・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[28]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（添付資料参照）

・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（添付資料参照）

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）

・サービスのセキュリティ強度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（添付資料参照）

・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

28　Data Free Flow with Trust（信頼性のある自由なデータ流通）。

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（添付資料参照）

・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（添付資料参照）

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持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　むすびと今後の展望

新型コロナウイルス感染症でより一層急務となった我が国のデジタル化を推進する過程では、技術的な利便性を追求するのみならず、安全・安心が脅かされないこと、すなわち適切なセキュリティ技術の開発と実践が肝要である。本 WG は、そのような背景の下、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ことが最優先課題であるとの共通認識に基づき、課題解決を実現するための方策を多角的に議論、整理した。その中心となるビジョンは産学官エコシステムの構築であり、具体的な方策は第２章と第３章に示した通り[29]である。

各方策の検討に当たっては、WG 委員内での活発な議論、オブザーバや幅広い外部有識者との意見交換、そして我が国の代表的な研究集会のイベントを利用した研究コミュニティでの積極的な議論を通じ、産学官エコシステムの実現に向けた礎を構築できたと評価している。第１章で述べたように、本分野の研究コミュニティは若いコミュニティであり、コミュニティ全体の発展に向けた道筋を大胆に模索できる点にアドバンテージがある。本 WG の取組をきっかけとして、今後も研究コミュニティとしての議論・意見交換が持続的になされていくこと、そして本 WG が提案する方策の実施と成功により、研究を担う博士課程学生、及びアカデミックな研究に従事する若手研究者が増え、また様々な場で研究構想や産学共同研究構想が提案され、我が国の産学官のエコシステムが重層的なものになること、さらにその結果として研究開発の国際競争力が大いに躍進することを期待したい。

本 WG では、取組が関係者の目に届くよう、可能な限り透明性が高い形式で実施した。具体的には議事概要の公開、ソーシャルメディアを用いた積極的な情報発信、研究集会におけるインタラクティブ性が高い意見討論を行った。そして、本 WG の取組を後に振り返り、紐解いてみる作業も重要であると考える。近い将来、本 WG が提案した方策を振り返ってみた際に、提案後にどのような方策が実践されたか、そして不足していた点は何であったかを明らかにすることは有益である。そのような振り返りをサポートするツールとして、「ワーキンググループ最終報告内容に係る将来のフォローアップに関して」を作成した。産学官エコシステムの確立に向けて、このツールが役立つようであれば望外の喜びである。

29　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）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。そのうち、1、2、6、7、9、10 に関し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 に関しては研究コミュニティ全体の発展で、8 に関しては第３章で、11 に関しては第２章で一部触れた。

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
（３）その他

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

令和２年 10 月 29 日
研究コミュニティとの意見交換

令和２年 11 月 25 日
中間報告とりまとめ
（研究開発戦略専門調査会にて報告・議論）

第 7 回　令和 2 年 12 月 23 日
（１）最終報告に向けた議論
（２）その他

第 8 回　令和 3 年 1 月 29 日
（１）最終報告に向けて
（２）その他

第 9 回　令和 3 年 3 月 12 日
（１）最終報告案について

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）

添付資料

「サイバーセキュリティ研究・産学官連携戦略ＷＧ最終報告案」（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～

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

第1章 はじめに

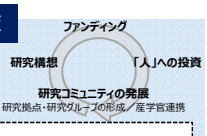
若く伸びている研究分野
- 国際的なトップカンファレンスへの論文投稿が2000年に比し約４倍以上。
- 我が国でも、2010年代に主な研究集会への参加者数が２倍以上に成長。
（サイバー空間の拡大と実空間との融合を背景に、国際的に存在感が高い暗号研究コミュニティの継続的でオープンな発展努力と様々な分野からの研究人口の流入。）

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	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

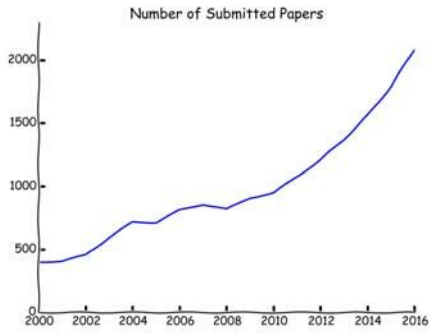
第4章 むすびと今後の展望

- 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。

サイバーセキュリティ研究に係る国際的な研究動向

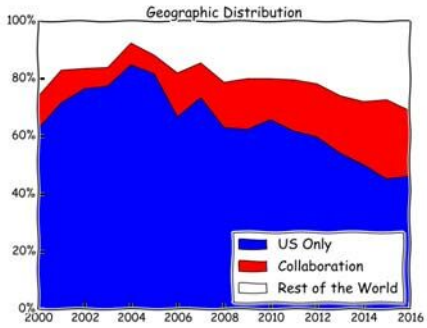
- 国際的に4つのカンファレンス（Top 4 conferences）が著名で、高い競争率の下、査読を経て、論文発表がなされる(※)。また、広範な研究分野のうち、暗号研究については「Crypto」や「Eurocrypt」が著名。
- 毎年、論文投稿数が増加しており、国際共著論文も増加。

論文投稿数



国別論文数（累積）

国際共著論文



4つのカンファレンスの論文発表動向（2000-2016年、ウェブサイトSystem Security Circus v2.0より）

URL: http://s3.eurecom.fr/~balzarot/notes/top4_v2/

4つのカンファレンス	IEEE Security & Privacy	IEEE Symposium on Security and Privacy. (IEEE: Institute of Electrical and Electronics Engineers)
	ACM CCS	ACM Conference on Computer and Communications Security. (ACM: Association for Computing Machinery)
	USENIX Security	USENIX Security Symposium. (USENIX: The Advanced Computing Systems Association)
	NDSS	Network and Distributed System Security Symposium
暗号研究	Crypto, Eurocrypt	(IACR: International Association for Cryptologic Research)

（※）カンファレンスでは研究成果はプロシーディング論文と呼ばれる形態で発表される。

どういった研究機関が参画しているか

- 4つのカンファレンスでは、米国の大学の存在感が非常に高く、次いで欧州の大学。カナダやイスラエルの大学も。
- アジアではシンガポール、中国、韓国の研究機関の存在感があるものの、日本の存在感は限定的。

所属別論文数（累積）

Affiliations

Rank	Name	Papers	Coverage	Size	Country
1	Carnegie Mellon University	174	83.8%	162	USA
2	University of California - Berkeley	154	92.6%	129	USA
3	Microsoft Research - US	138	69.1%	103	USA
4	Georgia Institute of Technology	102	64.7%	91	USA
5	Stanford University	100	77.9%	110	USA
6	University of Illinois - Urbana Champaign	81	63.2%	86	USA
7	University of California - Santa Barbara	80	66.2%	70	USA
8	University of Maryland - College Park	78	51.5%	69	USA
9	University of California - San Diego	77	63.2%	79	USA
9	University of Michigan - Ann Arbor	77	58.8%	81	USA

Legend:

- *coverage* : percentage of venues in which the institution had at least one paper
- *size* : number of Top-4 authors affiliated to the institution

（各地域の上位5研究機関）

欧州
- 18位　瑞ETH Zurich (53本)
- 20位　独Saarland Univ (51本)
- 25位　仏INRIA (47本)
- 独Ruhr-Univ Bochum (47本)
- 独TU Darmstadt (47本)

他地域
- 42位　加Univ of Waterloo (30本)
- 70位　イスラエルBar-Ilan Univ (15本)
- イスラエルTel Aviv Univ (15本)
- 加Carleton Univ (15本)
- 80位　イスラエルTechnion (14本)

アジア
- 53位　シンガポール国立大 (23本)
- 60位　中国・北京大(17本)
- 中国・清華大 (17本)
- 70位　韓国KAIST (15本)
- 90位　中国科学院 (11本)

日本
- 208位　IBM Research, Tokyo (3本)
- 244位　KDDI R&D Laboratories (2本)
- 336位　東北大、筑波大、東京大、電通大、慶応大、奈良先端大、九州大、産総研など (1本)

4つのカンファレンスの論文発表動向（2000-2016年、ウェブサイトSystem Security Circus v2.0より）

近年のトレンド

- 4つのカンファレンスで2019年は計435本の論文が発表(※)。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%、日本の研究機関が含まれる論文は5本。(2018年: 2本、2014年: 2本)
- 産学官連携論文が多いUSENIX Securityを例にとると、以下の通り。

【USENIX Security】 → *中国が躍進している。産学官連携論文が増えている。*

2014年

分数カウント

順位	国名	論文数	シェア
1	アメリカ	46.73	69.7%
2	ドイツ	10.35	15.4%
3	カナダ	2.11	3.1%
4	イスラエル	1.67	2.5%
5	中国	1.13	1.7%
6	フランス	1.00	1.5%
6	スイス	1.00	1.5%
6	オーストラリア	1.00	1.5%
9	オランダ	0.65	1.0%
10	ハンガリー	0.50	0.7%
11	シンガポール	0.33	0.5%
12	ギリシャ	0.20	0.3%
12	サウジアラビア	0.20	0.3%
14	アルゼンチン	0.14	0.2%

総論文数 67本

国際共著論文	19本	28%
産学連携論文	15本	22%

Microsoft 6本, Intel 2, RSA 2, Google 1, SAP 1, NEC米 1 等

2018年

分数カウント

順位	国名	論文数	シェア
1	アメリカ	60.44	60.4%
2	ドイツ	12.28	12.3%
3	中国	5.77	5.8%
4	イギリス	3.33	3.3%
5	オランダ	3.08	3.1%
6	カナダ	2.14	2.1%
6	フランス	2.08	2.1%
8	スイス	1.60	1.6%
9	ベルギー	1.43	1.4%
10	フィンランド	1.17	1.2%
11	イタリア	1.07	1.1%
12	スペイン	1.00	1.0%
12	ポルトガル	1.00	1.0%
12	イスラエル	1.00	1.0%
12	韓国	1.00	1.0%
16	オーストリア	0.50	0.5%
17	ポーランド	0.40	0.4%
18	ルクセンブルク	0.33	0.3%
19	チェコ	0.20	0.2%
20	オーストラリア	0.18	0.2%

総論文数 100本

国際共著論文	28本	28%
産学連携論文	19本	19%

Google 4本, Microsoft 2, Symantec 2, IBM 1, Samsung 1, Huawei 1, NEC米 1, Cisco 1, Siemens 1, GE 1 等

2019年

分数カウント

順位	国名	論文数	シェア
1	アメリカ	59.42	52.6%
2	ドイツ	13.34	11.8%
3	中国	9.62	8.5%
4	イギリス	7.38	6.5%
5	オランダ	3.81	3.4%
6	スイス	3.67	3.2%
7	イスラエル	3.27	2.9%
8	韓国	2.14	1.9%
9	オーストリア	2.07	1.8%
10	シンガポール	1.78	1.6%
11	フランス	1.14	1.0%
12	日本	1.00	0.9%
12	フィンランド	1.00	0.9%
12	ルクセンブルク	1.00	0.9%
15	イタリア	0.79	0.7%
16	チェコ	0.50	0.4%
17	ベルギー	0.32	0.3%
18	オーストラリア	0.29	0.3%
19	スペイン	0.22	0.2%
20	サウジアラビア	0.14	0.1%
21	カナダ	0.08	0.1%

総論文数 113本

国際共著論文	48本	42%
産学連携論文	30本	27%

Microsoft 3本, Symantec 3, Google 2(+2), IBM 2, Samsung 2, Baidu 2, Barracuda NW 2, Intel 1, Huawei 1, NEC米 1, NEC独 1 等 ()内は単独論文

(※) 集計はウェブサイト情報よりNISC 基本戦略第1グループが集計。分数カウントは、著者毎の所属機関を勘案して集計している。
日本参画論文は以下の通り: 早大(丸山/森ら)【IEEE Security & Privacy】、MPI-SP/CryptoExperts/Sorbonne/Rennes/ENS/NTT(ティブシ)【ACM CCS】、産総研(村上/川本ら)【USENIX Security】、TU Delft/NICT(井上ら)/横国大(吉岡ら)【NDSS】、NEC米/Columbia/Princeton/サイバーディフェンス研(コルツパルン)【NDSS】

近年のトレンド（Crypto）

- 暗号研究は、4つのカンファレンスと傾向が異なる。(日本の一定の存在感が確認できる。)
- なお、日本の研究機関で最も多く参画しているのはNTT。

【Crypto】 → *産学官連携論文が増えている。*

2014年

分数カウント

順位	国名	論文数	シェア
1	アメリカ	25.03	42.4%
2	イスラエル	7.25	12.3%
3	ドイツ	4.07	6.9%
4	日本	3.75	6.4%
5	フランス	2.98	5.1%
6	イギリス	2.42	4.1%
7	中国	2.15	3.6%
8	シンガポール	1.75	3.0%
9	スイス	1.08	1.8%
9	スペイン	1.08	1.8%
11	インド	1.00	1.7%
11	エストニア	1.00	1.7%
11	オーストリア	1.00	1.7%
14	韓国	0.95	1.6%
15	不明	0.67	1.1%
16	デンマーク	0.58	1.0%
17	オランダ	0.50	0.8%
18	カナダ	0.33	0.6%
18	イタリア	0.33	0.6%
20	オーストラリア	0.25	0.4%
20	ベルギー	0.25	0.4%
22	スウェーデン	0.20	0.3%
22	台湾	0.20	0.3%
22	マケドニア	0.17	0.3%

総論文数 59本

国際共著論文	32本	54%
産学連携論文	13本	22%

IBM 4本, NTT 3, Microsoft 3 等

2018年

分数カウント

順位	国名	論文数	シェア
1	アメリカ	33.44	42.3%
2	イスラエル	9.05	11.5%
3	フランス	5.65	7.2%
4	ドイツ	4.83	6.1%
5	デンマーク	3.68	4.7%
6	日本	3.63	4.6%
7	イギリス	3.16	4.0%
8	インド	3.08	3.9%
9	中国	2.59	3.3%
10	シンガポール	1.58	2.0%
11	ベルギー	1.27	1.6%
12	韓国	1.14	1.4%
13	スイス	0.95	1.2%
13	イタリア	0.95	1.2%
15	オランダ	0.70	0.9%
16	オーストリア	0.63	0.8%
17	イラン	0.57	0.7%
18	ノルウェー	0.50	0.6%
18	ポルトガル	0.50	0.6%
20	オーストラリア	0.33	0.4%
21	ルクセンブルク	0.31	0.4%
22	チェコ	0.25	0.3%
23	スペイン	0.20	0.3%

総論文数 79本

国際共著論文	43本	54%
産学連携論文	16本	20%

NTT 5本, IBM 4, Microsoft 2, Visa 1 等

2019年

分数カウント

順位	国名	論文数	シェア
1	アメリカ	39.05	48.5%
2	イスラエル	6.19	7.7%
3	日本	4.53	5.6%
3	中国	4.53	5.6%
5	デンマーク	3.60	4.5%
6	ドイツ	3.46	4.3%
7	フランス	3.30	4.1%
8	オランダ	3.08	3.8%
9	イギリス	1.72	2.1%
10	インド	1.45	1.8%
11	イタリア	1.40	1.7%
12	ベルギー	1.23	1.5%
13	カナダ	1.20	1.5%
14	スイス	1.13	1.4%
15	オーストラリア	1.00	1.2%
16	韓国	0.80	1.0%
17	シンガポール	0.63	0.8%
18	スペイン	0.50	0.6%
18	イラン	0.50	0.6%
20	ラトビア	0.33	0.4%
20	エストニア	0.33	0.4%
22	台湾	0.25	0.3%
23	ノルウェー	0.20	0.2%
24	オーストリア	0.08	0.1%

総論文数 81本

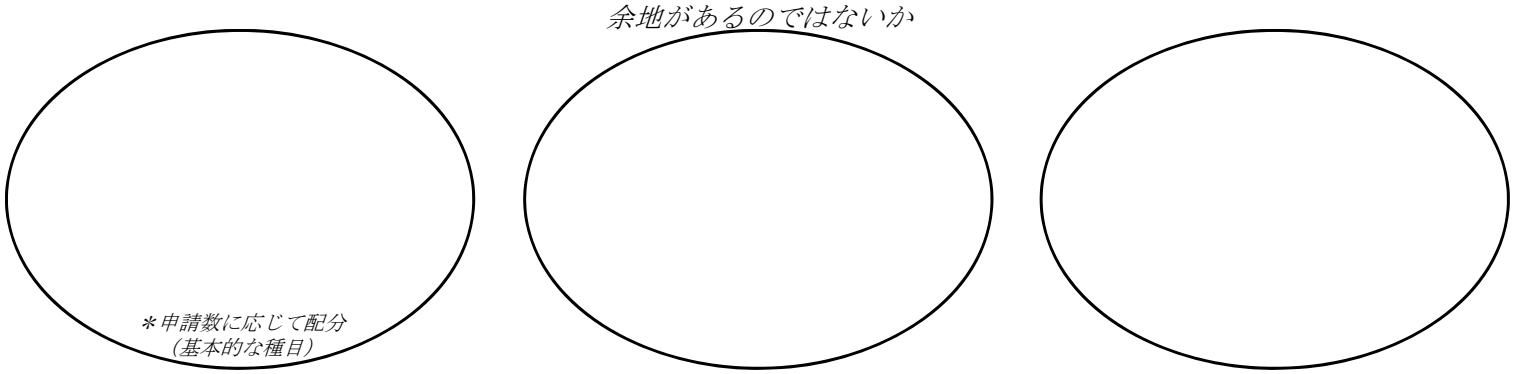
国際共著論文	44本	54%
産学連携論文	23本	28%

NTT 4本, Microsoft 4, NTT米 3, IBM 1, Visa 1, Qualcomm 1, Deepmind 1, Fujitsu米 1, NEC 1 等

(※) 集計はウェブサイト情報よりNISC 基本戦略第1グループが集計。分数カウントは、著者毎の所属機関を勘案して集計している。
日本参画論文の 13/17 はNTTが参画。他グループとしては、産総研、NEC/名大、NICT/日銀/横国大、東大/産総研。
NTTの共著者として以下が見られる: 東工大、産総研、兵庫県立大、NICT、京大、米U Maryland, 英UCL、スイスFHNW、ルクセンブルク大、ベルギーimec、イスラエルBar-Ilan U、印IIT、印・統計研究所、シンガポールNTU、中国科学院、中国・国家重点実験室

国・ファンディング機関のファンディングについて

研究コミュニティの発展
可能性をさらに高める
余地があるのではないか



研究者の自由な発想に
基づく研究（学術研究）
ボトムアップ型

政策課題対応型研究開発
トップダウン型

研究者が自由に研究課題を提案

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

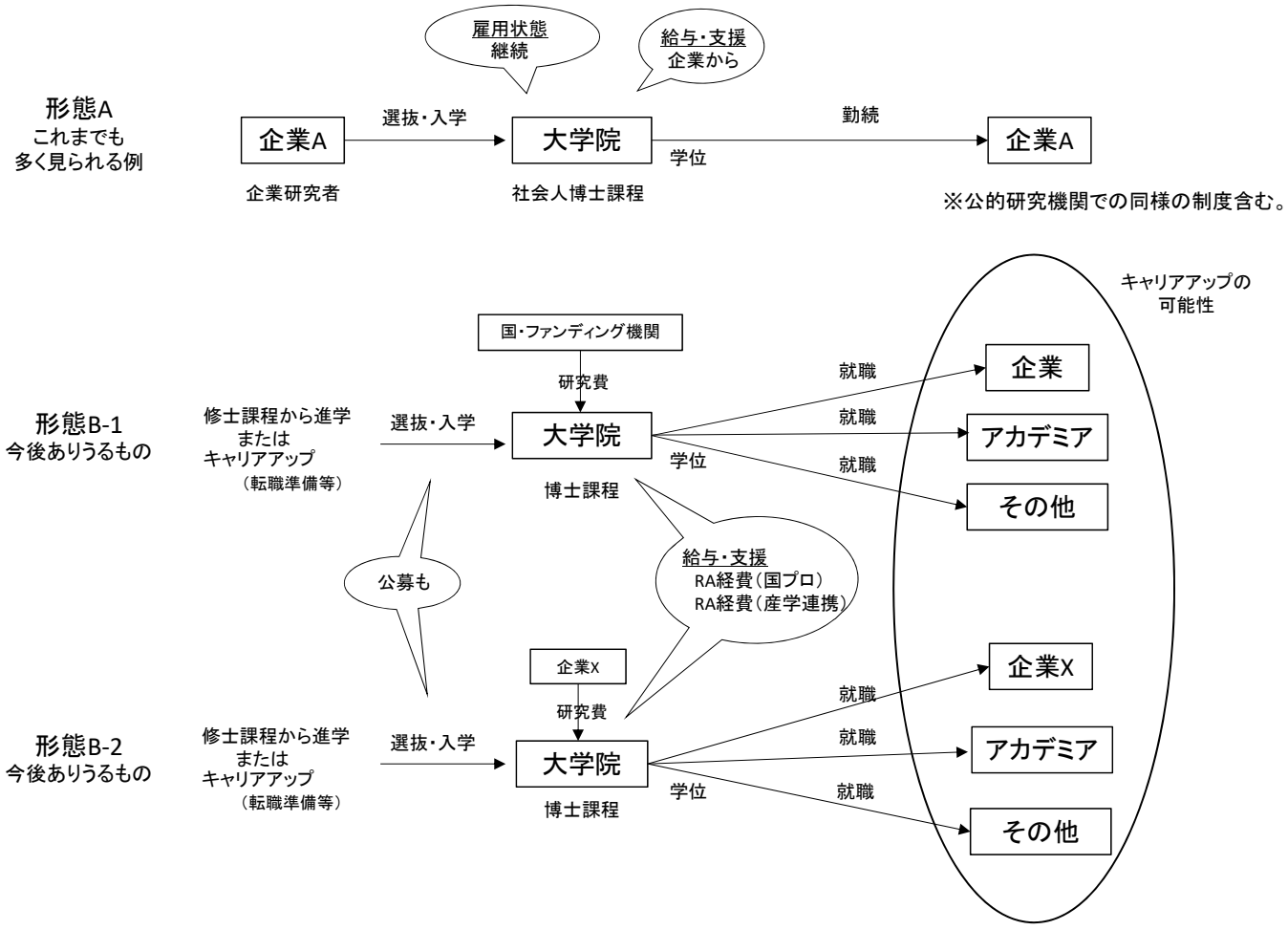
府省が進める研究開発プロジェクト

JSPS科研費

JST戦略的創造研究推進事業
（CREST/さきがけ等）
産学連携施策や研究拠点施策等
総務省SCOPE

SIP、総務省、NEDO　等

社会人を含む博士課程進学の様々な形態



海外における産学連携事例

lastline

攻撃等を検知するAI搭載のネットワークセキュリティ製品

Kirda ノースイースタン大学教授　Kruegel UCSB教授　Vigna UCSB教授

- 2011年、米大学の研究者3人で設立。3人のネットワークセキュリティ・マルウェア解析・攻撃についての研究、学問に根ざす厳格さ、革新的手法、情熱により会社のビジョンが作られている。（HPより）
- 2020年8月、ソフトウェアベンダ大手のVMware社により買収（買収額非公表）。

Censys

リアルタイムなデータ分析による脅威の可視化技術

Zakir Durumeric
スタンフォード大学助教
（設立当時ミシガン大学）

J. Alex Halderman
ミシガン大学教授

- 2017年、ミシガン大学のインターネットスキャナZMapの研究チームの一部が2人の経営者と組んで設立。可視化とリアルタイムデータで組織を守ることをミッションとしている。（HPより）
- なお、Durumeric助教はウィルス対策ソフトベンダAvastと産学連携の共同研究も実施。（Avast保有データを用いUSENIX Security '19で発表）

Bromium

仮想化技術によるマルウェア感染防止のためのエンドポイント向け製品

Ian Pratt
英ケンブリッジ大学
上級講師
（設立当時）

Simon Crosby
英ケンブリッジ大学
講師
（設立当時）

- 2004年、英ケンブリッジ大学コンピュータ研究所のPratt上級講師は、Crosby講師や教え子とともに米XenSource社を設立。同大学の研究プロジェクトで誕生した仮想化ソフトウェアXenを競争力のあるエンタープライズ製品にするため。
- 2007年、XenSource社は、米Citrix Systems 社に約5億ドルで買収され、Pratt氏は同社の副社長に就任。
- また、2011年、約140億円の投資を受けてPratt氏はBromium社を設立（カリフォルニア州）。仮想化技術（マイクロ仮想マシン）を用いた、マルウェア感染を阻止するエンドポイント向けのサイバーセキュリティ製品を開発。
- 2019年9月、米 HP社によりBromium社が買収（買収額非公表）。

intrinsic

サーバレス環境上のアプリのファイル等へのアクセス動作をセキュアに保つ技術

David Mazieres
スタンフォード大学
教授

Deian Stefan
カリフォルニア大学
サンディエゴ校(UCSD)助教
（現在）

- 2015年、スタンフォード大学コンピュータ科学科Mazieres教授とその教え子を含む創設者により、Intrinsic社が設立。
- Intrinsic社では、サーバレス環境上で動作するアプリが、正常にファイル等にアクセスするよう開発できる環境をソフトウェアで提供。
  これはスタンフォード大学における長年のプログラミング言語及びシステムセキュリティ分野の研究の成果。（HPより）
- 2019年8月、ソフトウェアベンダ大手のVMware社により買収（買収額非公表）。
- VMware社としては、本買収により、AWSやMicrosoft Azure等の成長するクラウドサービスに対して、それを支える基盤的な製品のセキュリティ機能を拡張する独自の知識・技術が獲得できたとしている。（記事より）

現状の強み分析のための研究領域の整理について

我が国の研究集会において過去5年に設けられたセッションであって、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

・過去5年間の電子情報通信学会「暗号と情報セキュリティシンポジウム（SCIS）」及び情報処理学会「コンピュータセキュリティシンポジウム（CSS）」の158セッションから、他セッション名で表せるものを除き58セッションに整理。ただし、我が国が一定の高い存在感を示している純理論系の暗号研究分野を除いたものが対象。
・上記58セッションを中分類、4つのフェーズ単位の小分類に割り当て、空白部を補足して以下の表を作成。
・さらに、各研究領域を基礎的要素となる保護対象や実装・評価及び対象分野に再整理・名称明確化を行った表が以下の通り。

	現状の強み分析のための研究領域の整理	中分類	小分類（フェーズ単位） 攻撃	検知（観測）	分析（解析）	対策
基礎的要素 保護対象	●ネットワークセキュリティ研究	通信系ネットワークセキュリティ	ネットワーク攻撃	●ネットワーク攻撃検知	●ネットワーク攻撃分析	●ネットワーク攻撃対策
			不正通信	●不正通信検知	不正通信分析	不正通信対策
		アクセス系ネットワークセキュリティ	不正アクセス	●不正アクセス検知	不正アクセス分析	不正アクセス対策
			DoS攻撃	DoS攻撃検知	DoS攻撃分析	●DoS攻撃対策
			悪性ドメイン構築	悪性ドメイン検知	悪性ドメイン分析	●悪性ドメイン対策
	コンピュータセキュリティ（プログラム保護）研究	プログラム保護	マルウェア	●マルウェア検知	●マルウェア分析	●マルウェア対策
			不正機能埋込	不正機能埋込検知	●動的解析 ●表層解析 ●プログラム解析 静的解析	●難読化
	コンピュータセキュリティ（Web セキュリティ）研究	●Webセキュリティ	Web攻撃	Web攻撃検知	●Web攻撃分析	Web攻撃対策
			悪性サイト構築	悪性サイト検知	悪性サイト分析	●悪性サイト対策
	アイデンティティ管理・認証研究	●認証	なりすまし攻撃	なりすまし攻撃検知	なりすまし攻撃分析	●ID管理 ●個人認証（生体認証含む） ●ユーザ認証 ●人工物メトリクス ●PKI
	データセキュリティ及びプライバシー保護研究	●プライバシー保護	プライバシー情報漏洩	プライバシー情報漏洩検知	プライバシー情報漏洩分析	●加工技術
		●個人情報保護	個人情報漏洩	個人情報漏洩検知	個人情報漏洩分析	個人情報漏洩対策
		●コンテンツ保護	コンテンツ不正流通	コンテンツ不正流通検知	コンテンツ不正流通分析	●情報ハイディング
	人的要素セキュリティ研究	人的要素セキュリティ（ユーザブルセキュリティ）	本研究は小分類（フェーズ単位）まで細かく分けられていないと思われるため、中分類までの項目を対象とする。			
実装・評価	実装セキュリティ（ハードウェアセキュリティ含む）研究	●暗号実装	●暗号実装攻撃	暗号実装攻撃検知	暗号実装攻撃分析	暗号実装攻撃対策
		●ハードウェアセキュリティ	ハードウェア実装攻撃	ハードウェア実装攻撃検知	ハードウェア実装攻撃分析	ハードウェア実装攻撃対策
		●OSセキュリティ	OS脆弱性攻撃	OS脆弱性攻撃検知	OS脆弱性攻撃分析	OS脆弱性攻撃対策
		●ソフトウェアセキュリティ	ソフトウェア脆弱性攻撃	ソフトウェア脆弱性攻撃検知	ソフトウェア脆弱性攻撃分析	ソフトウェア脆弱性攻撃対策
	セキュリティ評価・リスク評価研究	●セキュリティ評価	セキュリティ実装不備 セキュリティ設計不備 セキュリティ対策不備	●セキュリティ調査	●セキュリティ分析	●セキュリティ実装 ●セキュリティ設計 セキュリティ対策
		●リスク評価	脆弱性 リスク 脅威	脆弱性検知 リスク検知 脅威検知	●脆弱性分析 ●リスク分析 ●脅威分析	●脆弱性対策 ●リスク管理 脅威対策
対象分野	AIセキュリティ研究	●AIセキュリティ	↑ 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	
	IoTセキュリティ研究	●IoTセキュリティ				
	自動車セキュリティ研究	●自動車セキュリティ				
	サプライチェーンセキュリティ研究	●サプライチェーンセキュリティ				
	センサーセキュリティ研究	●センサーセキュリティ				
	モバイルセキュリティ研究	●モバイルセキュリティ				
		●FinTechセキュリティ	これらの研究は小分類（フェーズ単位）まで細かく分けられていないと思われるため、中分類までの項目を対象とする。			
		●オンラインバンキングセキュリティ				
		●クラウドセキュリティ				
		●計測セキュリティ				
		●産業制御システムセキュリティ				
		●無線セキュリティ				
		●メールセキュリティ				

ピンク背景は現状の強み分析を行った対象領域
水色背景は上記対象領域を構成する中分類・小分類の要素
●は上記の通り過去5年間で設けられた58セッション
研究開発戦略専門調査会第14回会合での事務局説明資料（資料3の整理例②）を基に作成

注1: 人的要素セキュリティ研究は近年の主要国際カンファレンスでセッションが設定されており、WG作業で提案され追加された。
注2: 分析資源や詳細化に限りがあるため、「対象分野」における研究領域のうち、一部対象にできなかったものがあるが、アカデミックな研究の広がりを考慮しつつSociety 5.0関連のものはできる限り分析対象とした。

実践的なサイバーセキュリティの研究分野　アカデミックな研究レベルの国際比較

(1)ネットワークセキュリティ研究領域

ネットワーク全般を保護対象としたセキュリティを研究する領域

中分類:	小分類:			
通信系ネットワークセキュリティ	ネットワーク攻撃	同検知	同分析	同対策
	不正通信	同検知	同分析	同対策
アクセス系ネットワークセキュリティ	不正アクセス	同検知	同分析	同対策
	DoS攻撃	同検知	同分析	同対策
	悪性ドメイン構築	同検知	同分析	同対策

国・地域	現状	トレンド	各国・地域の状況として特筆されるもの、及び、評価の際に参考にした根拠
日本	○	↗	早稲田大、NTT、横浜国立大、NICTなどが主要国際カンファレンスに採択され、プレゼンスが向上し、今後も期待できる分野の一つである（IoTセキュリティ・Webセキュリティと重複する部分あり）。NICTにおけるNICTERやNOTICEなど、NTTにおける悪性ドメインや悪性サイトに係る研究等、実践的かつ独自の研究が継続的に進められている。
米国	◎	→	伝統的に強く、世界をリードし、主要国際カンファレンスにおいても圧倒的に多数の発表を占めている。産業界でも強い。NSFやDARPA等から豊富な研究資金が供給され実データや大規模疑似データを用いて実用面でも理論面でも先進的な研究が継続的に実施されている。
欧州	◎	→	主要国際カンファレンスでは米国の◎には及ばないものの、研究拠点数や発表数を考慮すると中国や日本よりも強い。伝統的に強く、主要国際カンファレンスでも産業界でも強い。
その他（中国）	○	↗	主要国際カンファレンスでは、中国（清華大など）からの存在感が増している。量的に日本より若干リードしている印象。米国との共同研究だけでなく、単独の発表も増えてきている。

【研究領域の特徴】
ネットワークセキュリティ（侵入検知・攻撃検知）分野としては、1995年頃から存在するサイバーセキュリティの本流とも言える研究分野である。主要国際カンファレンスにおいて、ネットワークセキュリティは、必ずセッションが存在するが、2000～2005年頃のような盛り上がりはなく、2020年ではIoT/Webセキュリティ/Phishingといった周辺分野へ拡大している。ネットワークは、基盤となる技術ではあるが、DDoS対策などのように実課題がいまだに根強く残っているため、今後も継続する研究テーマであると考えられる。

(2)コンピュータセキュリティ(プログラム保護)研究領域

コンピュータを保護対象としたセキュリティのうちコンピュータを動かすプログラムを守る観点から研究を行う領域

中分類:	小分類:			
プログラム保護	マルウェア	同検知	同分析	同対策
	不正機能埋込	同検知	動的解析、表層解析、プログラム解析、静的解析	難読化

国・地域	現状	トレンド	各国・地域の状況として特筆されるもの、及び、評価の際に参考にした根拠
日本	△	↗	マルウェア分析や対策などでは、NTTを中心にTier2国際カンファレンス（ACSAC、RAID等）への採択など存在感を増しつつある。特に、2019年はACSACでの採択が2件あった。継続的に提供されているMWSデータセットの存在もあり、特に国内研究会では多くの研究がなされている。
米国	◎	→	Fuzzingなどを活用した脆弱性検知技術の研究が数多く行われ、ツール公開・利用が進んでいる。マルウェア分析技術は米欧が特に強く、サイバーセキュリティ研究の花形的研究であったため、存在感が高かった。学術研究から産業技術まで広くカバーかつ主導している。また、Lastlineのようなアカデミア発ベンチャーもあり、研究から産業へ昇華するスキームも整っていると言える。
欧州	○	→	マルウェア分析技術は米欧が特に強く、サイバーセキュリティ研究の花形的研究であったため、存在感が高かった。欧州・米国の有力大学の複数の研究室から成るiSecLabが2005年に発足して以来、現在も継続してマルウェア対策研究の主要な研究はiSecLabから出版され続けており、また後に米国で起業されたLastlineもiSecLabを運営する研究者によって誕生した。

【研究領域の特徴】
マルウェア分析そのものの研究領域自体は焦点が移りつつある印象であり、プログラム保護という考え方から対象がファームウェア・OS・CPU・ハードウェアと低レイヤかつ多様化したマルウェア研究にシフトしているように思われる。

評価の基準

【現状】◎：特に顕著な活動・成果が見えている　○：顕著な活動・成果が見えている
△：顕著な活動・成果が見えていない　×：活動・成果がほとんど見えていない
【トレンド】↗：上昇傾向　→：現状維持　↘：下降傾向　（直近2年程度の状況）

・実践的なサイバーセキュリティの研究分野とは、我が国における暗号と情報セキュリティやコンピュータセキュリティに係る研究集会で発表される研究分野のうち、純理論系の暗号研究分野を除いたもの。なお、暗号研究分野は、国際的に著名な研究集会（トップカンファレンス）においても、我が国は一定の高い存在感を示している。
・現状のアカデミックな研究レベルについて各国・地域の活動・成果状況をWGにおいて評価した。作業実施に当たっては、JST/CRDS「研究開発の俯瞰報告書」を参考とした。[x]

実践的なサイバーセキュリティの研究分野　アカデミックな研究レベルの国際比較

(3)コンピュータセキュリティ(Webセキュリティ)研究領域

コンピュータを保護対象としたセキュリティのうちコンピュータ上に構築されたWebサイトやその利用を守る観点から研究を行う領域

中分類:	小分類:			
Webセキュリティ	Web攻撃	同検知	同分析	同対策
	悪性サイト構築	同検知	同分析	同対策

国・地域	現状	トレンド	各国・地域の状況として特筆されるもの、及び、評価の際に参考にした根拠
日本	○	↗	NTTを中心に主要国際カンファレンスで発表されるようになってきており、その一つのNDSSやTier3国際カンファレンス（DIMVA）で2020年にBest Paperをそれぞれ獲得（NTT・早稲田大、NTT・横浜国立大）。特に攻撃研究で良い成果が出ているように思われる。Webからの脅威を観測するセンサーをユーザに配布して観測を行うWarpDriveプロジェクトが実施されており、その成果がTier2国際カンファレンス（RAID）でも採択。
米国	◎	→	欧米大学が特に強い分野であり、Webセキュリティに関するデータの収集などの知見は、日本より欧米の方が多く持っているように思われる。（本領域において、検索エンジンとWebブラウザはデータの観測点であり、主要なものは米国企業が中心に開発されたものであるため。）
欧州	◎	→	欧米大学が特に強い分野であり、Webセキュリティに関するデータの収集などの知見は、日本より欧米の方が多く持っているように思われる。欧州ではEU一般データ保護規則の施行に伴い、Web上でのプライバシー情報に関する研究（Webトラッキング、Cookieの取扱い、プライバシーポリシーの記述等）が促進されている。

【研究領域の特徴】
Webセキュリティでは、NDSSをはじめ、主要国際カンファレンスでは根強く人気が高いテーマである。米国を中心に近年ではcensorship（国家による検閲）やweb browser fingerprintingに関するプライバシー観点からの研究が盛ん。

(4)アイデンティティ管理・認証研究領域

人やモノを識別するアイデンティティを保護対象としその管理や認証を研究する領域

中分類:	小分類:			
認証	なりすまし攻撃	同検知	同分析	ID管理、個人認証(生体認証含む)、ユーザ認証、人工物メトリクス、PKI

国・地域	現状	トレンド	各国・地域の状況として特筆されるもの、及び、評価の際に参考にした根拠
日本	○	→	Tier2国際カンファレンス（AsiaCCS）には、暗号・認証系の発表がコンスタントにある。生体認証では、国際的にもNEC、日立、富士通等の産業技術が強く、主要国際カンファレンス（IJCB）でも一定の存在感。特に、NECはNISTコンペで精度での世界一位を取り続けている。
米国	◎	→	大学、企業いずれも非常に活発で、世界をリードし続けている。2020年の主要国際カンファレンス（IEEE S&P、ACM CCS、USENIX Security、NDSSの4大会議）では認証関連論文12件のうち4件が米国で、国別トップである。生体認証でも同様に国別トップである。GoogleやMicrosoftはOpenID ConnectやFIDOなどID連携、認証の標準仕様策定でも主導的に活動している。
欧州	○	→	大学等からの研究発表が活発。2020年の主要国際カンファレンス（4大会議）では認証関連論文12件のうち4件が欧州。生体認証では、仏国IDEMIAなど産業技術で大きなシェアを持つ企業があり、研究発表も活発。
その他（中国）	○	↗	2020年の主要国際カンファレンス（4大会議）では認証関連論文12件のうち2件が中国で、国別2位である。顔認証でSensetimeなどベンチャー企業が国際コンペで高い成績を出し、IJCBでも存在感を高めている。

【研究領域の特徴】
ID管理では、Microsoftなど米国企業を中心に分散ID /自己主権IDの研究が活発。

評価の基準

【現状】◎：特に顕著な活動・成果が見えている　○：顕著な活動・成果が見えている
△：顕著な活動・成果が見えていない　×：活動・成果がほとんど見えていない
【トレンド】↗：上昇傾向　→：現状維持　↘：下降傾向　（直近2年程度の状況）

・実践的なサイバーセキュリティの研究分野とは、我が国における暗号と情報セキュリティやコンピュータセキュリティに係る研究集会で発表される研究分野のうち、純理論系の暗号研究分野を除いたもの。なお、暗号研究分野は、国際的に著名な研究集会（トップカンファレンス）においても、我が国は一定の高い存在感を示している。
・現状のアカデミックな研究レベルについて各国・地域の活動・成果状況をWGにおいて評価した。作業実施に当たっては、JST/CRDS「研究開発の俯瞰報告書」を参考とした。[xi]

実践的なサイバーセキュリティの研究分野　アカデミックな研究レベルの国際比較

(5)データセキュリティ及びプライバシー保護研究領域

データ及びプライバシーデータを保護対象としたセキュリティを研究する領域

中分類:	小分類:			
プライバシー保護	プライバシー情報漏洩	同検知	同分析	加工技術
個人情報保護	個人情報漏洩	同検知	同分析	同対策
コンテンツ保護	コンテンツ不正流通	同検知	同分析	情報ハイディング

国・地域	現状	トレンド	各国・地域の状況として特筆されるもの、及び、評価の際に参考にした根拠
日本	◎	↗	主要国際カンファレンス（USENIX Security、ACM CCS、IEEE S&P、CRYPTO）やTier2国際カンファレンス（ESORICS、PETS）にも採択されており、2016年にACM CCSでBest Paperを獲得（NEC）。また日本からPETSのプログラム委員も出しており存在感がある。国内でも、匿名加工競技PWS Cupでの取組やSCIS・CSSの発表件数の増加など、顕著な活動が行われている。プライバシー保護ではNTTとNECが牽引し、関連技術である秘密計算は商用までこぎつけた。
米国	◎	↗	主要国際カンファレンス（USENIX Securityなど）では、米国からの発表が大半を占めており、欧州がそれに続く。
欧州	◎	↗	主要国際カンファレンス（USENIX Securityなど）では、米国からの発表が大半を占めており、欧州がそれに続く。

【研究領域の特徴】

プライバシー保護関連の秘密計算、秘密分散技術などの理論・実装論文がここ数年で世界的にも増加している。また、種々の実システムからの個人情報漏洩対策などがホットトピックとして議論されている。

(6)人的要素セキュリティ研究領域

人の行動や心理状態等の人的要素を考慮したセキュリティを研究する領域

中分類:	小分類:
人的要素セキュリティ(ユーザブルセキュリティ)	なし

国・地域	現状	トレンド	各国・地域の状況として特筆されるもの、及び、評価の際に参考にした根拠
日本	○	↗	主要国際カンファレンス（ACM CCS）やTier2国際カンファレンス（SOUPS、ACSAC）などに採択されている。また、サイバー系ではないが、ヒューマンコンピュータインタラクション分野の主要国際カンファレンス（CHI）でも発表されている。
米国	◎	→	カーネギーメロン大CyLab Usable Privacy and Security Laboratory（CMU CUPS）のCranor教授がユーザブルセキュリティの第一人者。Cranor教授がTier2国際カンファレンス（SOUPS）を2005年に始め、それ以来、米国を中心にユーザブルセキュリティに関して研究が盛んに行われている。CMU CUPSのOB/OGが米国の各種大学で研究室を持ち、多くの有力研究グループが生まれている。
欧州	◎	↗	独国の複数の研究チーム（Mathew Smith、Sascha Fahl/Yasemin Acar）を中心に、ソフトウェアの脆弱性と開発者に着目した研究成果が主要国際カンファレンスやヒューマンコンピュータインタラクション分野の主要国際カンファレンス（CHI）で多数発表されている。特に、Sascha FahlとYasemin Acarはユーザブルセキュリティ分野の賞（John Karat Usable Privacy and Security Student Research Award）を受賞している。

【研究領域の特徴】

近年盛り上がっている分野であり、主要国際カンファレンス（USENIX Security）では、2020年に複数のセッションが設けられ、本分野の論文3件がDistinguished Paper Awardを受賞した。エンドユーザを対象にした研究だけでなく、なぜ脆弱性を生んでしまうのかといった開発者の行動原理の解明などに着目した研究も出てきている。なお、本研究領域には、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が含まれる。

評価の基準

【現状】◎: 特に顕著な活動・成果が見えている　○: 顕著な活動・成果が見えている
△: 顕著な活動・成果が見えていない　×: 活動・成果がほとんど見えていない
【トレンド】↗: 上昇傾向　→: 現状維持　↘: 下降傾向　(直近2年程度の状況)

- 実践的なサイバーセキュリティの研究分野とは、我が国における暗号と情報セキュリティやコンピュータセキュリティに係る研究集会で発表される研究分野のうち、純理論系の暗号研究分野を除いたもの。なお、暗号研究分野は、国際的に著名な研究集会（トップカンファレンス）においても、我が国は一定の高い存在感を示している。
- 現状のアカデミックな研究レベルについて各国・地域の活動・成果状況をWGにおいて評価した。作業実施に当たっては、JST/CRDS「研究開発の俯瞰報告書」を参考とした。

実践的なサイバーセキュリティの研究分野　アカデミックな研究レベルの国際比較

(7)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

ハードウェアでの実装及びソフトウェア、OS、暗号技術の実装を行う際のセキュリティを研究する領域

中分類:	小分類:			
暗号実装	暗号実装攻撃	同検知	同分析	同対策
ハードウェアセキュリティ	ハードウェア実装攻撃	同検知	同分析	同対策
OSセキュリティ	OS脆弱性攻撃	同検知	同分析	同対策
ソフトウェアセキュリティ	ソフトウェア脆弱性攻撃	同検知	同分析	同対策

国・地域	現状	トレンド	各国・地域の状況として特筆されるもの、及び、評価の際に参考にした根拠
日本	○	→	主要国際カンファレンス（USENIX Security、IEEE S&P、ACM CCS）などにも採択されており、一定の存在感がある。暗号に関連した実装セキュリティ分野でも主要国際カンファレンス（CHES）でBest Paper Awardを受賞するなど日本が国際的に一定の強みを発揮している。国内でも電子情報通信学会にハードウェアセキュリティ研究会が発足するなど活発化の傾向が見られる。
米国	○	↗	近年は米国でも関心が急速に高まっており、論文投稿数・採択数とも増加傾向が見られる。特に、ハードウェアトロイについては盛んに研究されている。また、実装セキュリティに関連したベンチャー企業も一定数存在する。
欧州	◎	→	本分野は欧州が研究者規模の面で牽引してきた。特に、SpectreやMeltdownに端を発したCPUの脆弱性については、欧州の研究者を中心に盛んに研究され、世界的に追従されている。また、暗号に関連した実装セキュリティについても、ECRYPT II等のEUプロジェクトの成果が質・量ともに特筆される。
その他(中国)	○	↗	近年は中国でも関心が急速に高まっており、論文投稿数・採択数とも増加傾向が見られる。特に、CPUの脆弱性については、主要国際カンファレンスでの発表が一定数あると認識している。

【研究領域の特徴】

NECや三菱電機等の貢献によりサイドチャネル攻撃は2000年前後に日本でかなり進んだと思われる。現在、実装セキュリティ（ハードウェアセキュリティ）分野は世界的に拡大しており各地域で活発化している。この傾向はスコープに加える国際カンファレンス、主要国際カンファレンスでの関連論文数、参加者などがすべて増加していることから見て取れる。OSは今でも攻撃対象になっており、そのセキュリティを高める研究は続けられている。

(8)セキュリティ評価・リスク評価研究領域

システムの一部あるいは全体におけるセキュリティやリスクを評価する手法を研究する領域

中分類:	小分類:			
セキュリティ評価	セキュリティ実装不備	セキュリティ調査	セキュリティ分析	セキュリティ実装
	セキュリティ設計不備			セキュリティ設計
	セキュリティ対策不備			セキュリティ対策
リスク評価	脆弱性	同検知	同分析	同対策
	リスク	同検知	同分析	同管理
	脅威	同検知	同分析	同対策

国・地域	現状	トレンド	各国・地域の状況として特筆されるもの、及び、評価の際に参考にした根拠
日本	△	↗	日本も評価に関わる攻撃研究の存在感が出てきている。特に、AIスピーカーへの攻撃やWebサービスへの攻撃などが主要国際カンファレンス（USENIX Security、NDSS）で発表されている。なお、セキュリティ評価の標準化については、日本からISO国際標準化を働きかけISO/IEC27017（クラウドサービスに係るセキュリティ管理関連）が策定された実績がある。
米国	○	→	米欧が強く、特に大規模なセキュリティの調査や評価などは米欧の方が研究として実施されている印象がある。主要国際カンファレンス（IEEE S&P）では、米欧からコンシューマ向けIoT機器を販売する際のセキュリティ対策表記がどうあるべきかについて研究発表が2件なされ、攻撃技術に関するTier3国際カンファレンス（WOOT）も米欧の発表がほとんどである。
欧州	○	→	米欧が強く、特に大規模なセキュリティの調査や評価などは米欧の方が研究として実施されている印象がある。主要国際カンファレンス（IEEE S&P）では、米欧からコンシューマ向けIoT機器を販売する際のセキュリティ対策表記がどうあるべきかについて研究発表が2件なされ、攻撃技術に関するTier3国際カンファレンス（WOOT）も米欧の発表がほとんどである。欧州はセキュリティ評価に関する標準化活動を主導的に実施し始めている。

【研究領域の特徴】

網羅的なセキュリティ評価よりも、特定の新たな攻撃や現状調査を行い、それを結果的にセキュリティ向上につなげるというシナリオの研究が多い。日本では、実システムや製品に対する評価は控えられる傾向にあったが（ただし、生体認証に対する人工指による攻撃など先駆的な研究もある）、最近では適切な研究倫理考察、対応に基づき、実施されることが増えてきている。

評価の基準

【現状】◎: 特に顕著な活動・成果が見えている　○: 顕著な活動・成果が見えている
△: 顕著な活動・成果が見えていない　×: 活動・成果がほとんど見えていない
【トレンド】↗: 上昇傾向　→: 現状維持　↘: 下降傾向　(直近2年程度の状況)

- 実践的なサイバーセキュリティの研究分野とは、我が国における暗号と情報セキュリティやコンピュータセキュリティに係る研究集会で発表される研究分野のうち、純理論系の暗号研究分野を除いたもの。なお、暗号研究分野は、国際的に著名な研究集会（トップカンファレンス）においても、我が国は一定の高い存在感を示している。
- 現状のアカデミックな研究レベルについて各国・地域の活動・成果状況をWGにおいて評価した。作業実施に当たっては、JST/CRDS「研究開発の俯瞰報告書」を参考とした。

実践的なサイバーセキュリティの研究分野　アカデミックな研究レベルの国際比較

（9）AIセキュリティ研究領域

AIを対象としたセキュリティ及びAIが利活用されたセキュリティを研究する領域

中分類:　小分類:
AIセキュリティ　なし

国・地域	現状	トレンド	各国・地域の状況として特筆されるもの、及び、評価の際に参考にした根拠
日本	△	↗	ここ数年AIセキュリティに関連する分野に参入する研究者が上昇傾向にある。機械学習系の主要国際カンファレンス（AAAI、KDD、IJCAI等）では筑波大・理研をはじめとして、国内からの研究が定期的に採択されている。本分野におけるセキュリティ系の国際カンファレンスにおける国内研究者のプレゼンスは低い。九州大や筑波大が取り組んでいる敵対的サンプルの生成法に関する研究事例などが見られ、今後も拡大すると予想される。
米国	◎	↗	2013年頃より、GoogleやAppleに所属する研究者を中心に新しい概念が次々提案されてきた。大学、企業いずれも非常に活発で、企業はMicrosoftなどが発表。採択論文数の著者の約半数が米国であり、他国が主発表では米国は共著、米国が主発表では単独が多い。機械学習系の国際カンファレンスのみならず、セキュリティ系カンファレンスでもプレゼンスが高い。
欧州	○	↗	採択論文数の著者の約4分の1は欧州である。特にブラウンシュヴァイク工科大、ザールランド大をはじめ独国のプレゼンスが高い。実装関連の研究発表は欧州を中心に増加傾向にある。

【研究領域の特徴】
本分野は現在最もホットな研究分野の一つであり、どこの国も力を入れている競争が激しい分野である。主要国際カンファレンスでも複数のセッションが設けられることが多く、関連ワークショップ（AISecなど）も開催されている。セキュリティコミュニティのみならず、機械学習研究コミュニティが敵対的サンプルなどに関する研究を精力的に実施している。

（10）IoTセキュリティ研究領域

IoTを対象としたセキュリティを研究する領域

中分類:　小分類:
IoTセキュリティ　なし

国・地域	現状	トレンド	各国・地域の状況として特筆されるもの、及び、評価の際に参考にした根拠
日本	○	→	主要国際カンファレンス（NDSS）に共著で、Tier3国際カンファレンス（WOOT）に主著でそれぞれ採択されており、前者はDistinguished Paper Awardを受賞し、後者は高い被引用率を誇っている。国内の観測網（NICTのNICTER、JPCERT/CCのTSUBAMEなど）により、脆弱性発見等のIoTデバイスの分析も盛んに行われている。関連技術である暗号理論や実装セキュリティは日本が強みのある分野であり、利用が期待される軽量暗号とその実装等の分野では活動成果が見えている。さきがけや基盤研究において学術界での研究基盤もより整いつつある。
米国	○	↗	IoTサイバー攻撃が顕著になり、その攻撃実態の観測、IoTマルウェア解析や対策の研究が行われるようになった。攻撃の原因となる脆弱性の検知、脆弱性の原因となるソフトウェア開発における課題など、基盤となる技術に関する研究も進んでいる。
欧州	○	↗	研究の動向は米国に似るが、IoT機器のセキュリティ要件やガイドラインは各国が独立して策定しているものもあり、特定国でニーズが高い技術が出てくる可能性がある。英国・ブリストルやスペイン・サンタンデールなどスマートシティの実証実験が進んでいる。

【研究領域の特徴】
Mirai等の影響もあって、この数年注目度が高い領域であり、主要国際カンファレンスにおいてはセッションが必ず存在している。一方で、いろいろなテーマが出尽くした感もある。ただし、IoTと呼ばれるデバイスは日進月歩であり、今後出てくるデバイス（自動運転車、HEMS、医療なども含む）の新しい課題が出てくる可能性が常にある。

評価の基準
【現状】◎：特に顕著な活動・成果が見えている　○：顕著な活動・成果が見えている
△：顕著な活動・成果が見えていない　×：活動・成果がほとんど見えていない
【トレンド】↗：上昇傾向　→：現状維持　↘：下降傾向　（直近2年程度の状況）

・実践的なサイバーセキュリティの研究分野とは、我が国における暗号と情報セキュリティやコンピュータセキュリティに係る研究集会で発表される研究分野のうち、純理論系の暗号研究分野を除いたもの。なお、暗号研究分野は、国際的に著名な研究集会（トップカンファレンス）においても、我が国は一定の高い存在感を示している。
・現状のアカデミックな研究レベルについて各国・地域の活動・成果状況をWGにおいて評価した。作業実施に当たっては、JST/CRDS「研究開発の俯瞰報告書」を参考とした。

実践的なサイバーセキュリティの研究分野　アカデミックな研究レベルの国際比較

（11）自動車セキュリティ研究領域

自動車（特にサイバー空間と接続されるものや自動運転）を対象としたセキュリティを研究する領域

中分類:　小分類:
自動車セキュリティ　なし

国・地域	現状	トレンド	各国・地域の状況として特筆されるもの、及び、評価の際に参考にした根拠
日本	△	→	横浜国立大などが車載制御ネットワークに関する攻撃手法を報告。セキュリティの技術系カンファレンス（Black Hat Europe）では、横浜国立大・トヨタが共同発表。産業系の会議（Escar）では、日本の一定の存在感あり。日本の自動運転プラットフォームAutowareは国際的な評価も高い。ISO/SAE21434で自動車のサイバーセキュリティの法制化に係るUN規則をどのように実現するかを規定する規格を策定中であるが、その標準化を独国と推進。
米国	○	→	ミシガン大、テキサス大などが車載LANのセキュリティ強化技術（IDS、Firewall）をSAE Technical Paperなどに積極的に投稿。ニューヨーク大、サウスウェスト研究所及びミシガン大交通研究所の共同リサーチプロジェクトがソフトウェアアップデート技術の標準フレームワーク等を発表。SAE主催で自動車ハッキングコンテストを実施し積極的に自動車へのセキュリティ攻撃技術を議論する取組が進んでいる。
欧州	○	→	Fraunhofer SIT等の欧州研究所及び大学機関がEVITAなどの自動車セキュリティ研究開発プロジェクトに参加。CANメッセージ認証方式、車載LANのセキュリティ強化技術（IDS、Firewall）、ハードウェアセキュリティモジュール、車車間及び路車間通信におけるセキュリティ要件定義などの技術分野の研究発表。独国、仏国、英国を中心にISO/SAE21434標準化を推進。

【研究領域の特徴】
自動車セキュリティの研究は一定数存在するが、数は少ない。主要国際カンファレンスでセッションを組まれることもない。現状の自動車での研究はやり尽くされた感もあり、各社がフレームワーク提案に参入してきた数年前に比べると、だいぶ落ち着いてきた印象である。ただし、今後、自動運転のプラットフォームの普及が進むと、セキュリティ課題が顕著になる可能性がある。AIセキュリティやIoTセキュリティの側面を含むため、分野横断的領域であり、注目株である。

（12）サプライチェーンセキュリティ研究領域

サプライチェーン（特にITシステム・サービスに関するもの）を対象としたセキュリティを研究する領域

中分類:　小分類:
サプライチェーンセキュリティ　なし

国・地域	現状	トレンド	各国・地域の状況として特筆されるもの、及び、評価の際に参考にした根拠
日本	△	→	アカデミアでは、サプライチェーンセキュリティそのものが主題というよりも、サプライチェーンセキュリティ確保のための要素技術が主題とされることが多い。ハードウェアトロイ対策等の要素技術研究が行われている。日本での取組は、経済産業省のサイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）とSIPでの研究推進がある。
米国	○	↗	主要国際カンファレンスでも、サプライチェーン全体を対象としたセキュリティ研究というよりも、サプライチェーンセキュリティに関連する要素技術（ソフトウェア検証等）の研究が盛んに行われている。DARPAの研究プログラムにもサプライチェーンセキュリティが採択されている。ガイドライン策定（強制化）とブロックチェーン連携などの研究促進を実施している。
欧州	△	→	主要国際カンファレンスでも、サプライチェーン全体を対象としたセキュリティ研究というよりも、サプライチェーンセキュリティに関連する要素技術（ソフトウェア検証等）の研究が盛んに行われている。欧州は認証フレームワークの策定（法制化）を実施している。

【研究領域の特徴】
多様なサプライヤーから部品等を調達して、製品を製造することが一般的になり、サプライチェーンのセキュリティの重要性が高まっている。脅威としては、サプライヤーを対象としたサイバー攻撃により、情報の窃取、製造物への不正なソフトウェアの混入、生産活動停止・妨害などの脅威があり、サプライチェーンのセキュリティは、非常に重要になっている。また、ソフトウェア部品表であるSBoMを調達の要件とする場合が増加傾向にある。サプライチェーンセキュリティは、IoTやハードウェア、ファームウェア、OSなど様々な分野に関係する研究領域であり、関連要素技術など他の研究領域での研究と重複する研究があり得る。

評価の基準
【現状】◎：特に顕著な活動・成果が見えている　○：顕著な活動・成果が見えている
△：顕著な活動・成果が見えていない　×：活動・成果がほとんど見えていない
【トレンド】↗：上昇傾向　→：現状維持　↘：下降傾向　（直近2年程度の状況）

・実践的なサイバーセキュリティの研究分野とは、我が国における暗号と情報セキュリティやコンピュータセキュリティに係る研究集会で発表される研究分野のうち、純理論系の暗号研究分野を除いたもの。なお、暗号研究分野は、国際的に著名な研究集会（トップカンファレンス）においても、我が国は一定の高い存在感を示している。
・現状のアカデミックな研究レベルについて各国・地域の活動・成果状況をWGにおいて評価した。作業実施に当たっては、JST/CRDS「研究開発の俯瞰報告書」を参考とした。

実践的なサイバーセキュリティの研究分野　アカデミックな研究レベルの国際比較

（13）センサーセキュリティ研究領域

センサーやセンサーシステムを対象としたセキュリティを研究する領域

中分類:　小分類:
センサーセキュリティ　なし

国・地域	現状	トレンド	各国・地域の状況として特筆されるもの、及び、評価の際に参考にした根拠
日本	△	↗	主要国際カンファレンス（USENIX Security、ACM CCS、IEEE S&P）で散発的に活動成果が見られるが、絶対数が少なく、国際的に目立っているとは言えない。ただし、この2年で採択された実績があるため、上昇傾向とした。また、センサーへの各種攻撃によるセキュリティ評価などが国内外で成果が出てきている。ハードウェアセキュリティ研究会などの活動も影響していると思われる。
米国	◎	→	センサーの読取やセンサーへの注入に関するセキュリティの研究はミシガン大やワシントン大が強く、国際カンファレンスでも多数の論文がある。特に、ミシガン大では過去5年間だけでもセンサーセキュリティ関連で、主要国際カンファレンス（IEEE S&Pが4件、ACM CCSが2件）を含む多数の発表がなされており、同研究領域を牽引している。
欧州	△	→	主要国際カンファレンスでの発表件数やインパクトでは顕著な活動・成果はあまり見えていない。一部、レーダーに係るセキュリティでは、主要国際カンファレンス（USENIX Security）やセキュリティの技術系カンファレンス（Black Hat）で活動成果が見られる。また、音声認識のセキュリティでベンチマークコンテスト開催等の活動が見られる。

【研究領域の特徴】
メッシュネットワークの鍵管理やルーティングなどの基礎研究がある一方、センサー用ネットワークのためのSIMカードがバルク販売されるようになるなど実用面で材料が揃いつつある。また、自動車応用等も含め、各種センサーを含むシステムが増加傾向にあることから、センサーそのものもしくはセンサーネットワーク・システムに対する攻撃及び防御の研究は今後急速に伸びる可能性がある。実システムへの攻撃は、現状では米国が圧倒的に存在感があり、日本を除くアジアでは中国や韓国の顕著な成果が散見される。

（14）モバイルセキュリティ研究領域

モバイルデバイスやモバイルネットワークを対象としたセキュリティを研究する領域

中分類:　小分類:
モバイルセキュリティ　なし

国・地域	現状	トレンド	各国・地域の状況として特筆されるもの、及び、評価の際に参考にした根拠
日本	△	→	スマートフォンのハードウェアやソフトウェアを対象にした研究は増えておらず、ファームウェアやカーネル等の研究はほとんどない。端末外部の観測データからモバイル端末を保護する研究やプライバシー保護研究が目立つ成果。早稲田大・NTTを中心に、主要国際カンファレンスやTier2国際カンファレンス（AsiaCCS、SOUPS）に採択も日本の存在感は出せていない。NICT委託研究WarpDriveでAndroidが対象の実証実験が開始。
米国	○	↗	Android OSやAndroidマルウェアに関して米国を中心に研究が盛ん。2020年の主要国際カンファレンス（IEEE S&P、USENIX Security、NDSS）では本領域の論文数が11件であり、ファームウェア、カーネルなどスマートフォン内部のソフトウェア研究が増えていると思われる。
欧州	△	↗	2020年の主要国際カンファレンス（上記3つ）では本領域の論文数が6件であり、アプリを対象とした識別方法やセキュリティ機能の利用状況などの研究が多い。
その他（中国）	◎	↗	本領域は伝統的に中国の大学（復旦大、上海交通大等）から質が高い研究で主要国際カンファレンスに多数の論文が採択。2020年の主要国際カンファレンス（上記3つ）では本領域の論文数が5件であり、攻撃方法や脆弱性関連の研究が多いと思われる。

【研究領域の特徴】
Androidアプリの研究が主流だった分野であり、ここ10年で爆発的に進展して、サイバー系だけでなくソフトウェア工学系の主要国際カンファレンスでも論文が多数発表。研究のデータセット収集が比較的容易だったため、多くの研究者が本分野に参画。今でも、一定数の論文が主要国際カンファレンスで発表され続けており、手堅い分野。最近では、OSやファームウェア分析やエッジ環境下でのセキュリティに研究がシフトしてきている印象。また、新しいハードウェア機能が出てきているため、今後も重要な研究領域であると思われる。iOSを対象とした研究もAndroidに比べ少ないが行われている。

評価の基準
【現状】◎：特に顕著な活動・成果が見えている　○：顕著な活動・成果が見えている
△：顕著な活動・成果が見えていない　×：活動・成果がほとんど見えていない
【トレンド】↗：上昇傾向　→：現状維持　↘：下降傾向　（直近2年程度の状況）

・実践的なサイバーセキュリティの研究分野とは、我が国における暗号と情報セキュリティやコンピュータセキュリティに係る研究集会で発表される研究分野のうち、純理論系の暗号研究分野を除いたもの。なお、暗号研究分野は、国際的に著名な研究集会（トップカンファレンス）においても、我が国は一定の高い存在感を示している。
・現状のアカデミックな研究レベルについて各国・地域の活動・成果状況をWGにおいて評価した。作業実施に当たっては、JST/CRDS「研究開発の俯瞰報告書」を参考とした。

重点的な研究領域について

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は以下の通り。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。

安全・安心な社会基盤

デジタルインフラ（IoT、5G、クラウド、都市OS等）セキュリティ

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

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*

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）*

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

AIセキュリティ

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

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

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**

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基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*

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。

*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。
**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。
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。

※暗号研究分野の継続的な振興と国際的存在感の維持・向上等も極めて重要。また、科学研究費助成事業等による研究者の自由な発想に基づく研究は、発想・学理・シーズの源泉として極めて重要であり、引き続き推進されるべきものと考えられる。

実践的なサイバーセキュリティの研究分野　研究構想の具体例

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）

目標　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。

概要　分散型データの活用に際して重要となるプライバシーや非開示情報の保護について、分散させたままこれらを保護し、保護したまま制御、活用するための基盤技術の確立を目指す。加えて、そのような基盤技術を確立しつつ、様々なサイバー攻撃観測データを統合的に共有しアカデミックに分析し、より高度なセキュリティ対策を見出すための研究も併せて推進する。これにより、データの保護と活用を両立した信頼性のある自由なデータ流通（DFFT）に資する。

1．研究内容と背景

- データエコノミーが進展した社会においては、データの活用は、マーケティングなどの商業的な目的だけでなく、感染症対策などの公益的な目的にもつながり得るが、その際、プライバシーや非開示情報の保護を両立させることは極めて重要である。
- 特に、我が国の状況に鑑みると（メガプラットフォーマーがいない一方、分散的に多くのデータが存在すること等）、分散型データの活用が重要と考えられ、そのためには、セキュリティ技術により分散的に存在するデータに保護をかけること、保護したまま分散型データを制御、活用できることが必要であり、非構造化データを構造化することを含め、そのための基盤技術の確立を目指す。
- また、そのような基盤技術を確立しつつ、サイバー攻撃観測データに活用することで、多角的かつ多地点に分散した観測データを、匿名性やプライバシー・非開示情報を保ったまま統合的に共有し、アカデミックな分析を行い、より高度な対策を見出すことが可能となるため、これも併せて推進する。

2．具体的な研究例

セキュリティ分野の研究者と、機械学習やデータサイエンス分野等の研究者のコラボレーションによる研究実施が期待される。

A　プライバシー等を保護した社会的・経済的データの共有・分析基盤

個人情報や行動履歴等を活用したマーケティングやリコメンデーション、感染症対策などといった社会的・経済的価値創出に際して、Cの共通技術と連携しつつ、データ提供者が自己の情報をコントロールできる権利を維持し、必要な情報のみを共有・分析するための技術の研究を実施する。

例　・個人データを秘匿したままパーソナライズされたサービスや感染状況分析等へ活用する研究（分散型SNS、位置情報プライバシー 、検索可能暗号、Contact Tracing 等）
・データ所有者が自己の情報をコントロールできることを狙いとした研究（分散・自己主権ID、ブロックチェーン、Biometric Information Protection等）
・データを活用する多様な組織間で、データの相互運用を可能とし、円滑に活用できる環境の実現を狙いとした研究

B　非開示情報等を保護したサイバー攻撃観測データの共有・分析基盤

サイバー攻撃観測データについて、Cの共通技術と連携しつつ、情報交換の際にデータがどのように処理されるべきかなどを検討し、データの構造化、もしくは非構造化データのまま活用するための研究を実施する。また、多様な組織からサイバー攻撃観測データの共有が促進されるべく、インセンティブ設計技術の研究を実施する。

例　・サイバー攻撃に付随する多様なログ等を統合的に扱うためのデータの構造化を狙いとした研究
・データ提供者が、自身の提供するデータの量・価値に応じて適切なインセンティブ（見返りに分析できる他者のデータの量や期間等）を設定できるようにすることを狙いとした研究（ダイナミックプライシング、オークション理論等）

C　共通技術の深化・高度化及び新たな革新技術の創出

様々な分散型データに含まれる、一部もしくは全部のプライバシー情報や非開示情報等を秘匿したまま分析を可能にする技術など、データの保護・活用に関して、A、Bと連携しながら技術の深化・高度化を図るとともに、新たな革新技術の創出に挑む。その際、既存のプライバシー強化技術（PETs技術）の活用も念頭におきつつ、必要に応じて新たなPETs技術の創出を目指すことも含む。

＜保護・活用のための基盤技術＞
例　準同型暗号、秘密計算、（局所）差分プライバシー　（主に保護）
例　プライバシー保護データマイニング、Federated Learning (FL)、Privacy Preserving Machine Learning　（主に活用）

＜制御のための基盤技術＞
例　関数型暗号、ゼロ知識証明

3．想定する研究の進め方（PI人数規模のイメージなど）

A PI 5名、B PI 2-3名、C PI 7名　程度あるいはそれ以上

実践的なサイバーセキュリティの研究分野　研究構想の具体例

人工知能セキュリティ

目標　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。

概要　機械学習の重要性の高まりを受け、機械学習に立脚したシステムに対する情報セキュリティの重要3要素（機密性、完全性、可用性（CIA）の確立を根源的な狙いの一つとする。また、機械学習技術を高度に活用したセキュリティ技術の開拓を狙いとする。いずれも理論から応用に至る包括的な研究により基盤技術の確立を目指す。

1．研究内容と背景

- 将来の機械学習技術を高度に適用する社会においては、機械学習を活用したシステム全般に、より高度なレベルのセキュリティと信頼性が求められる。機械学習に対するセキュリティ強化を狙いとした研究が意欲的に研究され始めているが、包括的なフレームワークの確立には至っていない。
- 機械学習を応用したシステムを対象とし、機械学習に対する情報セキュリティの重要3要素---機密性 (Confidentiality)、完全性 (Integrity)、可用性 (Availability) を確立することを狙いとし、理論から応用に至る包括的な基盤技術に関する研究を行う。
- 機械学習を従来のセキュリティ対策技術に対して高度に応用した飛躍的な技術の開発研究、及びいわゆるオフェンシブセキュリティ（攻撃者視点の研究）のアプローチにより、攻撃者による機械学習の悪用がもたらす脅威と対策技術に関する基盤的研究を行う。

2．具体的な研究例

機械学習とセキュリティの研究者のコラボレーションによる研究実施が期待される。機械学習のCIA 確立は基礎研究を中心とし、機械学習のセキュリティ技術への応用は、応用研究を中心とする。

A　機械学習のCIA確立

＜機密性＞
機械学習が扱うデータ、及び訓練済みのモデルを保護することを狙いとした研究
例・ モデル抽出攻撃 (model extraction)と対策 （理論、応用）
・ データ再構築攻撃 (model inversion)と対策 （理論、応用）
・ プライバシー保護データマイニング技術（理論、応用） 基礎研究として差分プライバシーを含む秘密計算の機械学習への適用（理論、応用） 基礎研究として秘密計算関連研究全般を含む

＜完全性＞
機械学習を応用したシステムに対する悪意がある入力に対する保護を狙いとした研究
例・ 敵対的機械学習 (adversarial machine learning) に関する研究 （理論、応用）
・ 敵対的サンプル (adversarial example) の生成及び検出方法に関する研究（理論、応用）

＜可用性＞
MLaaS（machine learning as a service）のような機械学習アルゴリズムの出力を提供するクリティカルなシステムにおいて、不正なクエリの発行やデータ汚染が行われた際もシステムが影響を受けずに利用可能な状態を維持する技術の研究
例・ 機械学習アルゴリズムに対する不正な入力、パターンの発見、検出技術（応用）

B　機械学習のセキュリティ技術への応用

＜防御技術＞
本テーマは機械学習を高度に応用し、一般的なセキュリティ対策技術の飛躍的な性能向上を図る狙いとした研究である。スパムフィルタやマルウェア検出においてMLの適用が進むが、ML技術の進展に応じ、さらなる発展の見込みがある。また、攻撃技術として機械学習が使われた場合、いかに機械学習で対抗できるかに関する基礎検討を進める。
例・機械学習を用いたマルウェアの検出・分類技術
・機械学習を用いた悪性ウェブサイトの検出・分類技術
・機械学習を用いた侵入検知技術

＜攻撃技術＞
攻撃者が高度に機械学習を利用することで生じる脅威に関する研究
例・ 機械学習を用い、実際には存在しない画像、動画、音、テキストを巧妙に生成する技術と対策方法の研究
・ 本来秘匿されるべきデータに機械学習を適用することにより、高精度で推定するサイドチャネル攻撃の評価と対策方法の研究

3．想定する研究の進め方（PI人数規模のイメージなど）

AはCIA確立の元となる基礎研究を含め理論を中心に進める。B は応用を中心に進める。
A PI 5名　（理論4、応用1） B PI 5名（理論1、応用4）　程度あるいはそれ以上

実践的なサイバーセキュリティの研究分野　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に関する評価手法の確立＞

概略

共同研究先: インターネット企業（キャッシュレス決済などのサービス提供企業）、DXを進めるユーザ企業
実現の方向性: 既存の技術・システムにおけるセキュリティを深化させるもの

背景

想定する企業の潜在的あるいは顕在的なニーズとインパクト:（例えば事業の重要性や市場規模や波及効果や困難さ等に鑑みて、企業の事業や経営に携わる者が必要な資金（and/or 保有データ）を出したくなるか。）:

キャッシュレス決済、ポイント、クーポンなどの利用価値を提供するインターネット上のサービスでは、様々な業種のサービスと連携して利用者を増やし、多くの情報を収集して多様で付加価値の高いサービスを提供することでビジネスを発展させていく。

このようなサービスを支えるシステムのセキュリティ対策は益々重要となると考えられ、短中期的には、セキュリティを考慮した設計や脆弱性監査、セキュリティ事象対応等がなされると考えられるが、中長期的な観点からは、利用者のさらなる増大や連携サービスの様々な業種への拡大、サイバー攻撃の高度化・巧妙化等があっても、利用者の利便性等を損なわないまま、システムの盤石性をどう保てるかについて、社外の知見を得て対策を検討する関心は高いと想定される。

概要

共同研究により期待される成果:
1) 増大しうるリスクに対してセキュリティ対策が適切かつ効果的であることを定量的に示しセキュリティ強度を確認できる手法、2) 利用者のプライバシー保護等のセキュリティを確保した上でグループ企業や連携先などの社外とデータをセキュアに共有・活用できる手法、3) これらのセキュリティ強度と利用者の利便性がバランスしているか評価する手法、といったサービスのセキュリティ強度の評価について、共同研究により、科学的知見に基づく可能な限り客観的な評価手法を開発し、システム適用への道筋を得る。

共同研究の概要:
1) 大学等において、様々なサービスにおける複数のリスクを同時に考慮してコストを算出しつつリスクコミュニケーションを実施する研究で培われた技術に基づき、サービス間に存在する脅威やリスクをモデル化や定式化等することで、リスクを定量的に分析し、論理的にセキュリティ強度を評価する手法の構築を試み、提案する。
2) 大学等において、例えばプライバシー保護データマイニングなど複数のプライバシー保護技術を比較考慮しながら研究し、データをセキュアに共有・活用する手法のプロトタイピングを試みる。
3) 大学等において、ユーザビリティとセキュリティ・プライバシーに関する研究で培われた知見により、セキュリティ強度と利便性が両立したシステムとなっているかを分析し評価する手法の構築を試み、提案する。

共同研究の形態: 企業は資金及び自社のサービス・システムと研究グループをつなぐことができる人材を提供し、大学で研究員を雇用して研究する
共同研究に想定する期間及び規模: 3～4年、2400～4000万円/年、4～6名
想定される研究分野: セキュリティ評価・リスク評価、データセキュリティ及びプライバシー保護、人的要素セキュリティ

実践的なサイバーセキュリティの研究分野　産学共同研究構想の具体例

＜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＞

概略

共同研究先: ITベンダー企業（ソフトウェア開発企業（特にセキュリティソフトの開発を行う企業））
実現の方向性: 既存の技術・システムにおけるセキュリティを深化させるもの

背景

想定する企業の潜在的あるいは顕在的なニーズとインパクト:（例えば事業の重要性や市場規模や波及効果や困難さ等に鑑みて、企業の事業や経営に携わる者が必要な資金（and/or 保有データ）を出したくなるか。）:
ウイルス対策ソフトや資産管理ソフトなど、日本で利用される商用ソフトウェアの脆弱性がサイバー攻撃者によって悪用されている。ソフトウェアベンダーもコストをかけて脆弱性対策をしているが、より高度な攻撃対策を実装することが求められる。特に業務・サービスを止めずに運用することが求められる重要インフラにおいては、導入するソフトウェアの堅牢性や万が一の侵害時の悪用検知は重要視される傾向にあり、重要インフラ市場でも有効性が認められる対策であれば、製品の価値向上につながり、売上げに貢献できると想定される。

概要

共同研究により期待される成果:
ソフトウェアの脆弱性調査や対策の研究を行っている大学研究者との共同研究により、通常の市場サービスでは見つからないソフトウェアの脆弱性（ソフトウェアの動作等に係るもので例えば認証の不備で成立してしまう悪用など）を洗い出し、対策手法を検討する。プロトタイピングにより実装への道筋を得、製品の堅牢性を高めることに資する。さらに、攻撃者による製品機能の悪用検知や攻撃検知といった、よりプロアクティブな対策手法も検討する。なお、実施した脆弱性対策や悪用検知対策等に関する研究発表を可能とすることで大学側へのインセンティブを与えることも考えられる。（ただし、攻撃者に有益となる防御の工夫等、機微な部分については秘匿）。

共同研究の概要:
- 大学等においてマルウェアの動作特性の解析とそれを活用した対策の研究で培われた攻撃手法の分析能力と対策手法を使って、ダミーファイルを利用した悪用検知などのプロアクティブな対策手法を発案しプロトタイプ実装を試みる。
  （可能な限り実環境にて、攻撃研究を行っている研究者に攻撃演習を実施し、有効性を評価する。）
- 大学等においてファイルシステムやOSの仕組みに深くかかわる攻撃や対策といったハードニングにつながる技術研究で培われた知見を活かして、マルウェア等によるソフトウェアの悪用を監視したり、悪用から保護する対策機能（プロセスの保護、設定ファイルを含めた関連ファイルの保護強化など）のプロトタイプ実装を試みる。

共同研究の形態: 企業からは、資金及び共同研究要員を提供し、大学の研究員と合同で研究を実施する
共同研究に想定する期間及び規模: 3年、 ～2000万円/年、 2～3名
想定される研究分野: ソフトウェア脆弱性攻撃対策、攻撃の視点から知見を得る研究、マルウェア対策

実践的なサイバーセキュリティの研究分野　産学共同研究構想の具体例

＜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＞

概略

共同研究先: セキュリティベンダー企業
実現の方向性: 企業保有のデータを共有して学理に基づく分析を行うもの

背景

想定する企業の潜在的あるいは顕在的なニーズとインパクト: （例えば事業の重要性や市場規模や波及効果や困難さ等に鑑みて、企業の事業や経営に携わる者が必要な資金（and/or 保有データ）を出したくなるか。）:
テレワークの普及とともにクラウドサービス利用が増え、端末におけるセキュリティ対策が重要視されるとともに、端末利用におけるセキュリティリスク低減に向けた状況の分析・把握の需要が高まっている。そこで、セキュリテイベンダー企業が提供しているソフトウェア製品のPC端末の操作ログを活用することで、端末側でのセキュリティリスクの高い動作や、端末を操作する者が心理的に負担の高い状況にあることを分析・把握できるようにし、利用者のリスクを低減する。これにより、企業全体のリスク低減に寄与できるようにソフトウェア製品の機能が強化され、競合製品との差別化や新規サービス提供の機会につながりうると想定される。

概要

共同研究により期待される成果:
セキュリティベンダーより実際の環境にある各PC端末から収集した操作ログを提供することで、セキュリティ心理学的知見を有する大学にてセキュリティリスクの高い動作や、メンタルヘルス的に負担の高い状況を検知する条件を調査し、操作ログの分析手法を確立する。プロトタイピングにより製品の機能強化につながる実装への道筋を得るとともに、試行に協力してくれるユーザをセキュリティベンダーとともに獲得し、実環境での検証を行うことで精度を向上する。

共同研究の概要:
- 大学等において取り組まれているサイバーセキュリティ状況認識の研究で培われた行動分析的知見を使って、PC端末の操作ログからセキュリティリスクの高い状況につながると判断できる分析手法を発案しプロトタイプ実装と検証を試みる。
- 大学等において取り組まれているメンタル負荷などの研究で培われた心理学的知見を使って、PC端末の操作ログから心理的に負担の高い状況と判断できる分析手法を発案しプロトタイプ実装と検証を試みる。

共同研究の形態: 企業からは、研究費及びデータを提供し、大学にて研究員を雇用して研究を実施する
共同研究に想定する期間及び規模: 2年、 ～2000万円/年、 2名
想定される研究分野: 人的要素セキュリティ、OSセキュリティ

x xii