資料2

研究開発に関する今後の検討の素材
～研究・産学官連携の推進方策に係る議論～

令和2年7月

内閣サイバーセキュリティセンター（NISC）
基本戦略第1グループ

2020年1月時点での事務局の問題意識（SCIS2020での問いかけ）

現時点で思うところ…

研究

・いわゆるシステム・セキュリティ分野の研究はどう振興できるか

なお、暗号研究の持続的な振興も重要で、継続的に活発なコミュニティを自ら形成してきた一つの模範と思われる。

- 我が国の強みやポテンシャルは何か。若者や投資元にとっての魅力とは。社会的要請は。
- 科研費（小区分「情報セキュリティ関連」等）、さきがけ、CREST、SCOPE、NEDO、SIP等
- 推進に当たって何が課題か。分野の特質は何か。海外との違いは何か。
（技術的にドッグイヤーで様々な研究対象・手法があり実務対策を求める現場もある中でのアカデミアの役割、大学内での評価、国内での評価と海外での評価、研究基盤として研究室に一定のリソースが必要な領域、実データが必要な領域、他分野でみられるような共用の研究基盤とは何か、等）

産学連携

・日本のIT・セキュリティ業界（あるいはDX動向）の状況と展望、近年の産学連携・ベンチャーに係る環境、あるいは世界のIT・セキュリティ業界の動向を見越し、どのような産学連携が振興されうるか

Internationally visible

・情報と投資はボーダーを超える中、あるいは、頭脳と知識を集める拠点が研究競争力を持つ中、国際的な存在感や魅力ある環境をいかに構築できるか

インプットやご意見をいただければ

「技術戦略とは人を惹きつける産業やキャリアパスを見つけること」

SCIS2020: 電子情報通信学会における暗号と情報セキュリティシンポジウム。2020年1月に国内で開催され、800名以上が参加。

これまで、プレリミナリーな意見交換を有識者／研究者と実施してきた。

44件・50名

対象は企業事業系、企業研究者、大学研究者、公的機関研究者に渡る。

意見交換で挙げられた課題をプレリミナリーにまとめると、以下のとおり10程度となる。

振興に向けた課題①

- **博士課程学生の役割が海外と異なる。（海外（欧米）は社会を経験したドクターがフルタイムで給料を払われて研究戦力になっているが、日本はそういった研究室構造になっていない。）**

＜主なご意見＞

- 海外では、ポスドクや助教と同じようなプロセスで、ドクター学生が雇用前提で募集され、優秀な人材を選んで雇用している。【大学研究者】
- 海外では、博士課程の学生に給与を支払って、フルタイムで研究してもらっており、戦力になっているように見える。【企業研究者、大学研究者】
- 海外は（組織的に研究を進め）ゴールを明確にして、目的のために手段を選ばない。（カンファレンスに採録されるために、英語で執筆する人、プログラミングする人など役割分担する。）【企業研究者】
- 日本では博士課程学生が定員割れしており、社外人ドクター中心で学生がフルタイムで研究室に来ない。【企業研究者、大学研究者】
- 日本の学生が博士後期課程に進学しないのは、学費の問題が大きく、借金生活や先が見えない状況を不安に思っているためである。【大学研究者2名、企業研究者】
- 日本でも、博士課程学生が年600万円程度の給与をもらえるようになれば助かると思う。（事務局注: 日本において、研究費からRA（Research Assistant）経費を出せるといっても、金額は年200万円程度。）【企業研究者】

対応案の検討に向けて

- 他分野でも指摘されている課題と言える。
- 現実的にセキュリティ分野を中心にできることはないか。

振興に向けた課題②

- **日本では、ジャーナルでの論文成果(paper)が重視され、カンファレンスでの論文成果(proceeding)があまり評価されてこなかった。**

＜主なご意見＞

- 米国も欧州も、トップカンファレンスでの論文件数や外部資金を重視していて、トップカンファレンスでの発表が（国際的なあるいは企業に対する存在感となり）評価され、就職にも結びつく。【大学研究者2名】
- 欧州ではジャーナルでの成果がまだ少し評価されているが、カリフォルニア大学サンタバーバラ校などの米国はジャーナルでの成果を無視している。【大学研究者】
- システムセキュリティの研究成果は二番煎じではダメで、問題設定が新しいもの、インクリメントが相当大きいもの、時勢をとらえたものが評価されるが、海外の研究者はそういった論文をカンファレンスに投稿して結果を出している。【大学研究者】
- 日本では、ジャーナルでの成果は学位取得、人事評価、採用・転職時の評価に関係があるが、カンファレンスでの成果は評価されにくく、そもそもカンファレンスに投稿しない研究者もいる。【大学研究者3名】
- トップカンファレンスの一つであるUSENIXは、（査読も厳しく）国内ジャーナル10本分に相当すると考えられるが、実際にはそのように評価されない。ジャーナルの中には、投稿料さえ払えば無査読で掲載されるようなものも存在する。【大学研究者】

対応案の検討に向けて

- まずはWGや研究コミュニティで前向きな議論をしてもらうことが重要ではないか。
- また、本年春より、日本の研究コミュニティからトップカンファレンスに採録される論文数を増やすことを目的として、有志が投稿前の論文に対して助言する動きがあり、こういったコミュニティの自主的な取組を後押しすることも重要。
- 一定の議論が出てくれば、それにも応じて、以下などが考えられるのではないか。
  - その重要性・必要性につき国の政策メッセージを出す。（大学や研究コミュニティ内での評価に何らかの好影響を与えられる可能性。）
  - 国のファンディングプログラムの評価において、（IT・セキュリティ分野については）カンファレンス論文を実績として記述できるようにする。

振興に向けた課題③

- **いわゆるシステムセキュリティ分野について、アカデミアの役割は何か。（ITならではのスピード感が求められる一方、組織的に研究を行う手法が求められる。）**

＜主なご意見＞

- システムセキュリティ分野はITのイノベーションに影響されやすく、先読みが難しい分野であるため、スピード感とアンテナを張っておくことが重要である。そういった点で、日本は海外に後れを取っている。【企業事業系】
- システムセキュリティ分野は、理論研究である暗号系研究と異なり、（あるシステムを対象に）複数のポスドクやドクターで一定時間取り組んでようやくカンファレンスに採録されるような論文が書ける一方で、カンファレンスでは新規性が必要となる。【大学研究者3名】
- 事業への貢献や学術の発展など、研究の出口は研究者自身が意識すべきであるが、本質がわからずに研究しているなど、研究の出口を意識していない／できていない研究者も多く、システムセキュリティ分野では議論されていないように思われる。【企業研究者】
- 研究の出口が何であるかを求められて、自社の上層部にその都度説明させられていた。研究の出口は意識すべきであるものの、真面目に考えすぎると、クリエイティブ・イノベーティブなものが生まれにくくなってしまうこともある。出口と計画に縛られすぎない方が良い。【企業研究者】

対応案の検討に向けて

- WGや研究コミュニティで議論が深められることは、政策への示唆としても重要と考えられる。

振興に向けた課題④

- **いわゆるシステムセキュリティを学問として体系化しつつ振興していくことが必要ではないか。（なお、おそらく他国でも体系化まではなされていないと考えられる。）**

＜主なご意見＞

- システムセキュリティ分野は移り変わりが早いため、暗号分野のような体系化された教科書がまだ存在しない。【企業事業系、大学研究者】
- システムセキュリティについて、今のインシデント対応は、「現場で仕事を完遂してまた次の現場に向かう消防士」に近いが、本質的には、インシデント対応にも知識の蓄積が必要であり、医学のように、「現場があり、知識が学問として体系化され、その知識の蓄積を基に高等教育機関における人材育成がなされ、現場をやる人が育ち、基礎研究で新たな知のフロンティアを開拓する人も育つ」ような学問分野となるべきである。【企業研究者】
- システムセキュリティの基礎技術は、セキュリティ技術というよりネットワークなどのコンピュータサイエンス（CS）技術に関連が深いため、CSを学ぶことが基礎にあるべきである。【企業事業系】
- システムセキュリティ研究に必要なのは、（仕様書どおりに時間をかけてコーディングする外注ではなく）海外のように自らが試行錯誤しながら柔軟にコーディングする能力である。【企業研究者】
- 理論的な暗号分野と違い、システムセキュリティ分野は、ロボット分野と似ていて、論理的に数式で書けない、再現性や客観的な比較が難しいという特徴があり、アーキテクチャの思想から語る必要がある。【大学研究者】

対応案の検討に向けて

- WGや研究コミュニティで議論が深められることは、政策への示唆としても重要と考えられる。
- なお、分野・領域にかかる議論とも関連。

振興に向けた課題⑤

➢ **日本では、大学にセキュリティを主な専門にしている学科や研究室が少ない。**

＜主なご意見＞

- カーネギーメロン大学では、コンピュータサイエンスにセキュリティ分野が必ず存在し、2番目に多い。【大学研究者】
- セキュリティの研究室が多い大学は、東京電機大学、長崎県立大学、大阪大学、早稲田大学、立命館大学、横浜国立大学などである。【大学研究者2名】
- 日本では、大学によっては情報学科に一人もセキュリティを主に掲げる研究室がない場合もある。【大学研究者】
- 暗号分野には重鎮と言われる研究者はたくさんいらっしゃるが、サイバーセキュリティ分野は長い歴史があるわけではない。【大学研究者】
- SCIS2020には非常に多くの参加者がいて、学生にとってセキュリティ分野は魅力的であると感じているにもかかわらず、セキュリティを掲げる学科や研究室が少ない。【大学研究者】

対応案の検討に向けて

- SCISやCSSのように、セキュリティに関する学会・シンポジウムの参加者は若年層を含め増加しており、ITの進展に応じて、さらに研究ニーズが増えるポテンシャルあり。また、政策的要請や、AI戦略に基づく人材育成推進との機会も存在。
- 様々な研究者が大学内あるいはアカデミア内で具体的により大きな地歩を得るには何が重要か。欧米とは何が違うか。

振興に向けた課題⑥

➢ 海外や他分野で見られるような大型の産学連携が進む余地があるのではないか。

＜主なご意見＞

- 日本では、セキュリティ分野をはじめ、産業界と学術界の人材が流動しない。【大学研究者】
- 産業界とは違いアカデミアはデータもシステムも持っていないが、別の役割がきちんと存在するため、産学連携するとうまく噛み合うはずである。今は産学の間が分断されていることが問題である。【公的機関研究者】
- 海外の大学と共同研究を行う場合、セキュリティ分野でも、カーネギーメロン大学などは共同研究費が高い。【企業研究者】
- 企業は必要な技術を社外や海外から購入するだけで、自分たちで内製化しない。外注先のSIerはピラミッド型の下請け構造で人月仕事をしているのみである。企業内で技術力が向上しないため、クリエイティブな価値を生み出せない。【企業事業系】
- 産学連携するためには、将来に向けた「絵を描ける人間（事務局注：産学をマッチングする人や研究者自身）」が必要であるが、日本ではそういったことをできる人間が少ない。【企業事業系】
- 東京大学では、大学（シーズ）と産業界（ニーズ）をマッチングさせて、プロジェクトの立ち上げまでやってくれる取組を開始した。【企業研究者】
- システムセキュリティ分野でないものの、東京大学はmercari R4Dと5年間で10億円の「価値交換工学」に関する共同研究、ソフトバンクと10年間で200億円規模を目指す「Beyond AI 研究所」に向けた協定締結をそれぞれ行うことを発表した。【企業研究者】

- 事務局注：海外では、GoogleやMicrosoftなどの企業がトップカンファレンスで産学連携論文を発表している。日本でも、他分野では大型の産学連携が出てきているが、システムセキュリティ分野ではあまり見られないと認識。

対応案の検討に向けて

- 分野を問わず、国等の促進政策や施策が打たれており、事例も出てきている。
- セキュリティ分野での政策課題の検討とともに、具体事例が創出・把握され、共有されることが重要ではないか。

振興に向けた課題⑦

- **海外ではシステムセキュリティ分野のアカデミアがベンチャーを創設して産学連携を行う事例が見られるが、日本ではあまり見られない。**

＜主なご意見＞

- 海外では、Lastline、Arbor Networks、Censys、Coverityなど、トップカンファレンスに論文が通るような技術を世の中にどのように展開し、実際に使われる技術としていくかということで、産業界を見据えているが、日本ではそういった状況になっていない。【大学研究者、企業研究者、企業事業系】
- 米国は人材が流動する。大学で良いものができたらスタートアップを立ち上げ、しばらくしたらまた大学に戻る。スタンフォード大学のように、大学籍のまま起業することが多い大学もある。【公的機関研究者】
- 日本にはスタートアップが少なく、大学の研究者が兼業でベンチャーを立ち上げると、良くないように聞こえてしまうイメージがある。【企業研究者2名】
- 社会的に必要とされているにもかかわらず、日本では、セキュリティ製品やサービスでお金を儲けるのが難しい。【企業研究者2名】
- 海外は研究成果を売り物・ビジネスにするが、その多くを政府が購入している。他企業や海外の評価を気にする日本はこういったことが得意ではないが、正のスパイラルになるように、政府が方向性を出せると状況が変わっていくと思う。【公的機関研究者】

- 事務局注：従前に比し、様々な分野で、日本でも大学発ベンチャーのIPO・M&Aが珍しくなくなり、起業する学生も見られるようになっている。

対応案の検討に向けて

- 分野を問わず、国等の促進政策や施策が打たれており、事例も出てきている。
- セキュリティ分野での政策課題の検討とともに、具体事例が創出・把握され、共有されることが重要ではないか。

振興に向けた課題⑧

➢ **コミュニティ内あるいは産学で、研究のためのデータを共用することが困難である。**

＜主なご意見＞

- コンピュータセキュリティシンポジウム（CSS）と併催しているMWS（マルウェア対策研究人材育成ワークショップ）は、企業がデータセット（生データや加工データ等）を提供し、大学などからの参加者が研究や当日のコンペティションに使用できる取組であり、2008年から始まっている。産業界と大学が連携する良い取組であるが、日本ではそれでもデータを提供するのに躊躇してしまい、コミュニティ内で横展開がなされていない。【大学研究者、企業研究者2名】
- レベルの高い研究成果を出すには、データセットも高度化が必要であるが、企業としてはセンシティブなデータや最新のデータを提供するのは難しい。【企業研究者】
- ユーザ企業はユーザデータを保有しているが、プライバシーの問題があるため、データを提供する際のガイドラインなどがあると良い。【企業研究者】
- 標的型攻撃の場合、攻撃を観測する仕組みがなく、データを取得できなくて困っている。【大学研究者】
- 参考として、WarpDrive（Web媒介型攻撃対策技術の実用化に向けた研究開発）案件では、ユーザの許諾を得た上で閲覧データを取得し、取得したデータは受託7社で共有する仕組みになっており、研究発表などにも使用できるという成功事例がある。【大学研究者】
- データが収集されることも重要であり、産業界も含めて、データ収集する土壌をつくることも重要である。【公的機関研究者】

対応案の検討に向けて

- 課題⑥や⑦と関連する内容であり、産学連携やベンチャーにかかる議論の中で具体議論されることも重要ではないか。

振興に向けた課題⑨

➢ **セキュリティ分野では、研究コミュニティ全体で、ファンドを活用できていないのではないか。**

＜主なご意見＞

- セキュリティ研究者が文部科学省系のファンド（JSTやJSPS、科研費など）を必ずしも獲得できていない。コミュニティ内に、他分野で見られるようなまとめ役が必ずしもいない。【大学研究者2名】
- さきがけプロジェクトの研究領域「IoTが拓く未来」のようなセキュリティに関わるファンドがあっても、残念ながら、セキュリティ研究者の応募は多くなかったようだ。【大学研究者、企業研究者】
- ファンド関連の申請書を作成するのは論文を1本仕上げるのと同じくらい大変であるが、多額の予算を必要としない場合、時間と手間をかけるインセンティブが小さくなる。【大学研究者】
- 複数組織でファンドを獲得する場合、大学より企業の取り分が多い。（事務局注: SIP課題では、企業が代表研究機関を務めることが専ら。）【大学研究者】
- 国プロを受託した企業は、委託元省庁など（事務局注: 総務省、経済産業省、NICT、NEDO等）が指定した安い単価でしか人件費を計上できないため、実際に要した人件費に対して損失が出てしまう。そのため、受託企業は損失の出ない外注費などの割合を増加せざるを得ない。【公的機関研究者】

対応案の検討に向けて

- 様々なファンディングがバランスよく活用され、研究コミュニティが発展することは重要。
- まずはWGや研究コミュニティで前向きな議論をしてもらうことが重要ではないか。
- 他分野では、コミュニティが適切な発信やコミュニケーション等を行うことで、継続的にファンディングが設定・獲得されるような分野が見られる。

振興に向けた課題⑩

➢ **セキュリティ分野には、大学を巻き込んだ研究拠点施策がない。**

＜主なご意見＞

- ドイツ政府機関が国立研究所として設立したCISPA（Helmholtz Center for Information Security）には、Saarland大学を中心とした500人のセキュリティ研究者が在籍している。【大学研究者、企業研究者】
- CISPA自体が研究テーマを決めて、ドイツ政府が年間50億円も出資している。欧州全体から優秀な研究者が集まっていて、人が人を呼ぶ状況である。研究者は給与も高く、ベンチャーも立ち上げている。トップカンファレンスでは、米国と同レベルの採択数になっている。【企業研究者、大学研究者】
- 日本国内や海外に取組をアピールする観点からも、文部科学省の「光・量子飛躍フラグシッププログラム（Q-LEAP）」のようなランドマーク的なプロジェクトがシステムセキュリティ分野にも立ち上げられることが望まれる。【大学研究者】

- 事務局注: SCIS2020のように若手を含む参加者が増えている学会は多くなく、他学会と比べて、コミュニティがより良い方向に向かって行くのに必要な環境が存在すると考えられる。

対応案の検討に向けて

- 様々なファンディングがバランスよく活用され、研究コミュニティが発展することは重要。また、大学という場を活用した研究開発の遂行は重要。
- まずはWGや研究コミュニティで前向きな議論をしてもらうことが重要ではないか。

振興に向けた課題⑪

➢ **日本では、どのような研究が回避すべき攻撃研究かわからず、研究としてどこまで許されるかわからない。**

＜主なご意見＞

- 暗号分野では、コミュニティ内に既にコンセンサスがあり、暗号方式を攻撃しても、罪に問われないし、迫害もされない。【企業研究者】
- トップカンファレンスでは、サイバー攻撃に関する研究発表もあり、海外は攻撃研究に対するノウハウがある。攻撃研究は技術として重要であり、防御技術を向上させるためにも必要である。【公的機関研究者】
- 日本のシステムセキュリティ分野では、攻撃研究を行うことが難しく、攻撃を助長してしまうとして、実際に攻撃した研究者が逮捕された事例もある。【公的機関研究者、企業研究者】
- クローニングやリバースエンジニアリングなど攻撃研究の定義や範囲が曖昧で、日本の研究者はどこまで攻撃研究を実施できるのかがわからない。（事務局注：弁護士に相談する研究者もいるが、事例ごとの判断が必要であり、一概に決められないとのこと。）【企業研究者】

対応案の検討に向けて

- 昨年、コンピュータセキュリティ研究会が「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」を作成して、攻撃研究などに倫理的に配慮させる啓発活動を行う動きあり。