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
第１回会合　議事概要

1．日時
令和２年７月 29 日（水）　10:00～12:00

2．場所
Ｗｅｂ会議形式での開催

3．出席者（敬称略）

（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
	森 達哉	早稲田大学理工学術院　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

（事務局）	山内 智生	内閣審議官
	吉川 徹志	内閣参事官
	上田 光幸	内閣参事官
	小西 良太郎	参事官補佐
	太田 陽基	参事官補佐
	中尾 康二	サイバーセキュリティ参与

（オブザーバー）	鵜飼 裕司	研究開発戦略専門調査会　委員
	木村 康則	研究開発戦略専門調査会　委員
	高島 洋典	国立研究開発法人科学技術振興機構　研究開発戦略センター　（木村委員同行）
	井上 眞梨	国立研究開発法人科学技術振興機構　研究開発戦略センター　（木村委員同行）
	総務省	
	文部科学省	

4. 議事概要

（1）ワーキンググループについて

事務局より資料の説明後、委員による本ワーキンググループの主査の互選が行われ、森委員が主査として選任された。また、「研究・産学官連携戦略ワーキンググループの運営について」が案のとおり決定された。

（2）研究・産学官連携の推進方策に係る議論について

専門調査会で議論された振興に向けた課題について、適宜事務局から議論促進のための関連資料の説明を受けつつ意見交換が行われた。今回、主査の提案に基づき以下の課題につき議論が行われ、意見の概要は以下のとおり。

課題1　博士課程

- 情報系など、博士課程に進学すると就職できなくなるということではないであろうと思う。オフィシャルにそのようなメッセージを発信することは大事。
- 企業への就職において、博士課程学生は希望する研究テーマと合わないと、優秀だとしてもジョブマッチングが難しい傾向。企業で採用するのは研究職でも修士課程卒がほとんどなのが現状。
- 博士課程に進学すると、キャリアの出口が限られる。学生はキャリアの出口をよく見ている。博士課程学生は使いにくいイメージを持たれていることも問題であると思う。
- 情報・セキュリティ系では、就職できるのに極端に心配する状況。心配しなくて大丈夫というメッセージが重要。
- RA 経費について、月額 20 万円や年額 200 万円が主とのことだが、情報系では企業に就職するともっと好待遇。金銭的な理由も博士課程進学可否の決め手の一つであるため、RA 経費の上限を柔軟に考えられると良い。
- 学生にとって将来のキャリアプランが重要である。博士課程学生にも、どんなことでもやる人とやりたいことだけやる人がいる。どんなことでもやる人であれば企業側も広く受け入れられるが、自身の専門に拘りすぎると受け皿が狭くなる。企業側のニーズを知ったキャリアプランが望まれる。
- 社会人ドクターはニーズが高い。毎年数名は入ってくるが、個人的なコネクションがほとんどである。実際にどれくらい大学に来る必要があるのか、など学位取得までの実態がわかるとさらに希望者は増えるのではないか。周知のためのプロモーションや情報公開が重要。企業と受け入れる側の大学のマッチングができるようになると良い。
- 企業からすると、一度でも社会の荒波にもまれた経験がある人の方が受け入れやすい印象がある。自身が社会人ドクターを取得したのは、特に国際的なアカデミアの場で話に入ることさえできなかったという経験からであり、必要になってから取得しても良いのではないか。修士卒で就職してから社会人

ドクター取得というキャリアパスも有効であると考える。

- 高処遇に関するコメントが他の委員から述べられた件に関して、すべての企業が同じ状況であるとは限らない。企業の待遇に関する客観的なデータがあった方が良い。
- 東京大学の UMP-JUST の取組例で、企業と情報理工学系研究科をマッチングしているが、有能な学生を能力に見合った給料年額 600 万円で雇用とある。企業が学生のバイトに週 20 時間で月額 50 万円、年額 600 万円を出す例がある由。
- セキュリティは実学であると考えるが、大学のセキュリティ研究と企業のそれが必ずしも一致していない。コンピュータサイエンスの基礎力があって幅広く活躍できる情報系の学生は国内外で引く手あまただが、必ずしもセキュリティ専門ではない。セキュリティだけに拘りすぎるとうまくいかない。
- 社会人ドクターは人材育成、基礎と応用の連携、産学連携などいくつかの課題に対してソリューションになりえる。何らかの形で制度化ができると良い。
- 博士課程学生や社会人ドクターは東京大学の事例もあり、国の支援など具体的に実現できることはあると思われる。

（以上、秋山委員、須賀委員、高島氏、高橋委員、永山委員、本間委員、森主査、山内委員、山田委員、吉岡委員、事務局（五十音順））

課題 4　学問体系化

- 企業におけるセキュリティ研究は、医学で言う臨床に相当する部分が中心であるのに対し、大学や国研は基礎研究の割合が大きく、たとえば博士課程学生の就職においてミスマッチが起こりやすい要因とも考えられる。大学や国研で基礎研究を安定して続けられるポストを増やさないと、臨床と基礎研究の両輪を育てていくことは難しいのではないか。
- Information Technology Curricula という ACM と IEEE 発行の IT・コンピュータサイエンス系の学士課程向けカリキュラムのガイドラインがあり、参考にするのはどうか。セキュリティ分野だけでなく IT・コンピュータサイエンス全般を俯瞰して記述されている。全体の中にセキュリティ要素が染み込んでいるものなので、セキュリティだけを切り出さない方が良いと思う。
- 医学では大学で基礎研究も臨床も両方実施している一方、サイバーセキュリティでは、両方実施している大学は少ない。大学の情報システムセンターには研究に使えそうなデータがあるが、人が少なく論文を書けないほど忙しい。米国のカーネギーメロン大学には CERT があり、研究だけでなく実践の役割も強いのかもしれない。
- 情報処理学会でも、カリキュラム標準 J17 を策定している。J17 では、情報セキュリティのカリキュラムが追加されている。このカリキュラムは学生をどのように教育すれば良いかの参考になる。
- 医学のアナロジーは興味深い。医学の基礎研究は臨床とつながるところがあるように思うが、セキュリティの実践は、個々の基礎研究分野の技術とだいぶギャップがあるように思う。その中で、トップガン人材とジェネラリストのどちらを育てるのかといった視点も学問体系化をはかるうえでは必要では

ないか。
- 医学では、医学部は大学病院と連携していて、セキュリティとは少し状況が異なる。体系化は重要であり、フランスやドイツなどの体系化が得意そうな国をはじめとして、世界でもトライされているが、うまく整理されていない。

（以上、秋山委員、高橋委員、中尾参与、本間委員、山内委員、吉岡委員（五十音順））

課題６　産学官連携
- 支給額が初年度から徐々に減らされる大学へのファンディングがある。最初の数年は良いが、それ以降は減額され、大学の自助努力による民間資金での補填が求められている。この施策の結果として想定どおり産学連携は増えているのか。
- 数百万円規模の共同研究はコネクションやリクルートが主目的と考えられる。一方、大型のものは、研究部門を自社で抱えずに大学に委託するケースが存在する。これらの選択が各社の判断で行われている。
- 大型の共同研究が増えているという肌感覚はある。従来、経営層には、社内の研究部門に投資するという考え方があったが、オープンイノベーションも増えており、ある意味、社内と社外の競争になっている。また、ベンチャー企業への投資・買収もある。大学から見ると、ベンチャーが競争者になる。
- セキュリティに関する大型の産学共同研究の例として、日立-慶應義塾大学の共同研究がある。研究テーマの具体例としては、複数の SOC で集めてきた知識を集約する「分散 SOC」などがある。
- 大型の産学官連携の例として英国のブリストル大学はスマートシティ構想で国と連携している。設計段階から関わり、数百億円規模である。独国でも同様の例がある。スマートシティのようなアプリケーションがあると大型化できる。
- 研究や産学官連携のエコシステムをまわす上で、ボトルネックとなるところを修正していく必要がある。また、連携していく上で、企業のニーズと大学のシーズがマッチしていないという課題がある。

（以上、高橋委員、中尾参与、永山委員、森主査、山田委員（五十音順））

引き続き議論を継続することとなった。

（３）分野・領域に係る議論について

事務局から資料の説明後、意見交換が行われた。意見の概要は以下のとおり。

- 日本の CSS や SCIS のセッションに出てこない、トップカンファレンスにしか存在しない分野もある。また、日本の強いところだけでなく、日本の弱いところであってもどうするか考えるべき分野があるのでは。

- 強みをどのように測るのかを考える必要がある。カンファレンスでの発表件数もあるし、研究を実施する上で法制度的に有利なこともある。日本が世界と戦えている分野はどこか、戦えていない分野はどこか。戦えていないならば、その理由の分析も必要である。
- 他分野では、日本の独自性を創出しようとした結果、本当にインパクトある研究テーマから逸れてしまっている事例がある。そうならないようにすべきである。また、現在の状況だけでなく、将来的にどの分野で強くなりたいかも考える必要がある。
- トップカンファレンスを見ていると、重要なイベントやインシデントが発生したとき、それに対する世界の研究者の動きはとても早い。体系化しているわけでもないのに、いつの間にか一つのジャンルになっている。例えば、最近は世界的にリモートワークが進んでいるが、これに伴うセキュリティへの影響なども既に取り組まれているかもしれない。
- 重点化すべき領域論とは別に、まだ分からない新興領域自体を政策的にどう扱うか規定する政策例がある。
- 重点分野とされている場合、そのキーワードは既に活発に研究されており、資金・研究リソースが大規模に投資される段階である。一方、その前の段階にある斬新な研究分野をつくる・見つけることも重要である。
- 短期で成果を出す実践的研究と長期で出す基礎研究の両方を意識すべき。短期ものはフットワークが重要であり、例えば AI や量子などがある。セキュリティだけ切り出すのは難しいという意見があったが、実践的な領域ではその通りと思う。一方で、セキュリティ全体を見る長期的な基礎研究との両立が必要である。
- 重点化の軸について、セキュリティには外部脅威と内部脅威の考え方がある。外部脅威では、攻撃者を意識するが、内部脅威では、技術的にセキュリティをどう向上させるかという基礎技術に注目されることが多い。両者を分けて考えると良いのでは。
- サイバーセキュリティでは、攻撃者からいかに守るかが重要である。分野・領域としても、多岐にわたり幅も広い。すべての領域を狙うと、議論が発散する懸念がある。企業のニーズなどを考慮して、日本の強みだけでなく、弱みも検討すべき。

（以上、秋山委員、荒木委員、中尾参与、永山委員、本間委員、山内委員、山田委員、吉岡委員、事務局（五十音順））

以上を踏まえ、今後適宜委員からの発表も交え、議論を継続することとなった。

以上