

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2回会合 議事概要

1. 日時

令和2年8月6日(木) 10:00~12:00

2. 場所

Web会議形式での開催

3. 出席者(敬称略)

(主査)	森 達哉	早稲田大学理工学術院 教授
(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
	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

(事務局)	山内 智生	内閣審議官
	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
	中野 孝一	主査
	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
	寺田 真敏	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) 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。前回に続いて、主査の提案に基づき以下の課題のまとまりで議論が行われ、意見の概要は以下のとおり。

##### 課題5 セキュリティ看板、課題9 ファンド活用、課題10 大学巻き込み拠点

- 国内では 20 年前に暗号分野の研究拠点が作られた事例があると聞いた。今後、直接関わった方から話を聞いて参考にすることも有益と考える。
  - ファンド活用に関し、CREST やさきがけでは、IT の中にセキュリティが含まれていて、セキュリティが主になる領域が存在しないため、セキュリティの深い議論ができない。セキュリティが主になる領域が必要である。
  - さきがけの IoT 領域はセキュリティ分野のコミュニティからの採択者が多いとは言えない。セキュリティが主になる領域があれば、研究が活性化する。
  - セキュリティ分野単体で領域が立ち上がりにくい。文科省関連では、サイエンスとしてのセキュリティをどう考えるか重要ではないか。
  - 文部科学省の担当部局も JST も、研究コミュニティに意見を聞きながら、重点領域を策定していく。セキュリティ分野のコミュニティとして、ファンディング機関と連携していくと良いと思う。
  - セキュリティについては、文部科学省の審議会でも議論しており重要と認識。セキュリティとしてどのような分野・技術が重要であるか、本 WG での意見も参考にしたい。
  - CREST やさきがけの話があったが、総務省や経済産業省などにもファンドがある。双方の位置づけの違いは何か。
  - 総務省や経済産業省にはいわゆる国プロがある。また、総務省 SCOPE では基礎的な研究も行われていると認識。文科省はあらゆる分野の基礎研究を所掌している。
  - 総務省は情報通信分野を所掌し、文科省と比べれば情報通信産業やネットワークを利用するユーザを対象とした研究開発に寄ったところはある。一方、大学など多様な視点からの研究課題も重要であると認識し、NICT や大学との研究連携も積極的に進めている。
- (以上、総務省、高島氏、本間委員、森主査、文部科学省、山内委員、山田委員、事務局、(五十音順))

##### 課題2 プロシーディング、課題3 アカデミアの役割、課題8 データ共有、課題11 攻撃研究

- 論文件数は研究推進能力を測るために使われるものであり、自分はジャーナルかプロシーディングかを意識したことがない。いずれを書くべきか気にする研究者がいるなら、記入要領の記載ぶりを検討した方が良い。
- 国際会議のプロシーディングで発表して、それを手直した論文をジャーナルに投稿するといったこともある。プロシーディングを書いて良いと明記し

ても、応募者が、成果の二重カウントなどを心配する恐れがある。そのあたりの考え方を整理して注意書きとして提示する必要があるかもしれない。

- 研究提案申請にプロシーディングの成果も書いて良いなら、書けるようにしてほしい。ただ、評価自体は、評価する側が判断することである。なお、大学内の評価に関し、大学によっては、論文の件数だけを見ているところもある。
- 審査の現場では、ジャーナルとプロシーディングで区別していないことが多いと感じる。

(以上、高島氏、永山委員、本間委員、山内委員 (五十音順))

#### 課題7 ベンチャー

- 吉岡委員の資料に記載されている Lastline 社は研究を主軸とした大学発のベンチャーであり、成功事例である。
- セキュリティ分野のベンチャーが成功するか否かについて、米国やイスラエルなどでは、国がベンチャーを積極的に採用することで、ビジネスが軌道に乗り、成長することが多い。国の調達の仕組みなど、状況の異なる日本では難しいかもしれないが、海外でセキュリティベンチャーが成功している理由としてこの点が大きいのではないか。
- 事務局資料 P6 のセキュリティ系ベンチャーの事例とそれ以降の一般的なベンチャーの事例には違いがあるのではないか。一般的なベンチャーは、起業（ビジネス）を志向しているが、P6 のセキュリティ系ベンチャーは、研究に軸足を置いた教授のベンチャーであるため、起業が目的ではなく、研究に資するデータを集めるなどを志向しているのではないか。
- ベンチャー起業は、大学の先生が立ち上げるものと、学生が立ち上げるものがある。ベンチャー起業が身近にあれば周りにも波及する。セキュリティの研究コミュニティにはあまり事例がなかったと思われるが、今後どうするか考えるべき。
- 起業家はあまり語らないが、実際の起業の当事者にはお金や人など考えることが本当にたくさんある。なぜ海外のアカデミアではセキュリティ分野でベンチャーがあるのか当事者の本音を知りたい。
- 米国の事例では、先生が大学に籍を置きながら、ベンチャーも立ち上げている。例えば、スタンフォード大学では、2年間ベンチャーに専念できる制度がある。すなわち、米国では先生が大学と企業を比較的自由に行き来でき、またそのような仕組みも整っているように見える。
- FinTech 分野のスタートアップ企業には、論文を積極的に発信することで、企業価値や信頼性を高めていくという相乗効果を生み出している企業もある。

(以上、荒木委員、鶴飼氏、木村氏、須賀委員、森主査、山田委員、事務局 (五十音順))

これまでの議論を踏まえ、取り扱う課題を設定しつつ集中的に議論をすることとなった。

## (2) 分野・領域に係る議論について

吉岡委員、秋山委員から発表資料の説明後、意見交換が行われた。意見の概要は以下のとおり。

- 韓国はスマホ関連の研究でトップカンファレンスに採録されているが、サムスンの影響が大きいのではないか。また、米国はプロセッサやファジングツールを開発していて、関連する研究も活性化している。例えば、プロセッサの脆弱性が見つかり、プロセッサの脆弱性の研究が活性化する。一方で、日本はこうした関連分野が産業として弱い面があり、どうしても研究領域としても弱くなってしまう。
- 網羅性を確保しようとする分類学・整理学での議論が必要だが、各委員の専門カバーにも限界があるため、1年で一定の結論を得るには少々の偏りは仕方ない面もあるだろう。ただ、こういった側面もあることに留意しながらも、最善と思われる結果を目指すよう進めるのが重要と思う。
- 日本と海外のセキュリティ製品を比較すると、最先端で尖がっていて素晴らしい海外製品でも、いざ実環境に導入するとトラブルが発生するなど、品質面に問題があるケースもある。一方、日本製品は一般的に品質が高く、運用面に配慮されていることも多い。品質や、実運用に配慮する細やかさはセキュリティ分野においても日本の強みになるのではないか。
- 研究レベルで優れている技術と、実際の運用で有効な技術というのはギャップが存在すると思う。運用のレベルで役に立つ技術に関する検討がさらに重要になっていると思う。NICTでは、複数のセキュリティアプライアンスを同時に利用して、運用レベルでの比較、評価をしている。
- 強みを検討する上で、日本と海外の研究のレベルの比較で現在の強みを分析する手法があると思うが、それに加えて、研究コミュニティや日本社会の特性をもって「強みになりうる」という分析もあると感じた。
- これまではセキュリティ分野での強みの話が中心であったが、例えば、TCP/IP や DNS などのアーキテクチャが開発された頃は必ずしもセキュリティを考慮していなかったと思う。日本が HCI 分野に強いのは良いこと。HCI 分野など、日本が強い他分野とコラボレーションして、その分野のアーキテクチャを研究するときに、一緒にセキュリティも考えると良い。
- 産学が一体となって成果を出すためには、ゴールが何か腹を割って話さないといけない。学術のインセンティブは論文成果だが、企業では、研究者なら論文も成果になるが、事業部はそうでない。
- 世界的に普及する技術を目指すなら、日本特有の事情・環境に特化した技術では市場が日本にしかなく難しい。
- HCI のトップ会議である ACM CHI ではユーザブルセキュリティに関する研究も増えてきている。日本のリードがある HCI 分野と連係して設計段階からセキュリティを検討する方法がありうる。
- CPU やスマホ等の日本が強くない・製品を持っていない分野では、日本で研究しようとしても、開示される情報が不足していてブラックボックスになり、直接戦うのは難しい。一方、日本は暗号理論が強いが、出口へのマッチング

が難しい。暗号の強みを活かせるの良いのだが。

- 産と学のギャップについて、企業では論文を書いても評価されない。一方で、産が学に求めることは学問体系化や研究の俯瞰である。
- (日本が産業として強みを持たない) OS や CPU の分野は、学術的にも日本が弱みであり、圧倒的に海外についていけない。
- 国際会議で戦うには日本の研究者の英語のアカデミックライティング・アカデミックな思考法のレベルが不足している。海外の大学所属の研究者からアドバイスをもらうようになって、Tier1 の国際会議にも採録されるようになった部分もあると感じる。
- 攻撃のローカライゼーションが進展し、例えば日本や台湾でしか観測できない攻撃があるということは考慮が必要である。米国や欧州でも日本への攻撃を観測していないわけではないが、自国への攻撃解析の粒度には及ばないところがある。日本の強みとして輸出できるような技術を育てる必要がある一方、自国で自給自足すべき分野もある。
- 本議論では、日本の強みを検討したり、軸で並べて重点化を検討したりしようとしているが、今後の産学連携がどのようなものになり得るかという観点も軸としてあると感じた。その際、一口に産業界と言っても、相手がユーザ企業、ベンダー企業、インターネット企業で事情は異なり、それを分けつつ考える必要がある。

(以上、秋山委員、荒木委員、鵜飼氏、須賀委員、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))

これまでの議論を踏まえ、議論の整理を行いつつ集中的に議論をすることとなった。

以上