

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5回会合 議事概要

1. 日時

令和2年9月29日(火) 15:30~18:00

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
	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

(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
	中野 孝一	主査
	中尾 康二	サイバーセキュリティ参与
	八剣 洋一郎	セキュリティ指導専門官

(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)
	内閣府 科学技術・イノベーション担当 総務省	

4. 議事概要

(1) 研究・産学官連携の具体に係る議論について

前回に引き続き、研究領域、産学共同研究、日本の強み分析のまとめ案等に関し、具体の議論が行われ、適宜事務局から関連資料の説明を受けつつ意見交換・フリーディスカッションが行われた。概要以下のとおり。

研究領域の具体例

- 事前に委員より提案がなされた研究領域の具体例のアイデア（資料 1-1）について、WG の集合知として一定数を提示していくため、検討を進めるべきアイデアとして、DFFT、人工知能、プライバシー保護等が挙げられた。その上で、ブレインストーミング的にフリーディスカッションがなされた。
- DFFT に関するアイデア（通し番号 1）については、データ流通は今後大切である、プライバシー保護技術は暗号分野と相性が良く日本の強みになりうる、領域が広いため多少細分化した方が良い、提案されている複数の研究例について関連があると良い等の意見があった。
- 人工知能に関するアイデア（通し番号 5）については、社会的に重要である、可用性に相当する学習モデルの客観的評価や完全性に相当するアルゴリズムが正しく実装されているかの証明もスコープに含まれるべきである、機械学習とセキュリティ双方の研究者が少ない、まだ取り組まれていないブルーオーシャンもありシナリオを考えるべき、さきがけやCRESTでの取組との差別化が必要である等の意見があった。また、文科省による信頼される AI の取組、産総研や IPA による AI 使用時の安全性やブラックボックス評価に関する取組が紹介された。
- プライバシー保護に関するアイデア（通し番号 2）については、DFFT に関するアイデアと関連する可能性がある等の意見があった。
- また、Connected Car セキュリティ、サプライチェーンセキュリティ、レクリエーション暗号に係るアイデアについても説明があり、WG だからこそ面白いものを出すのが良い、WG らしさを考える必要がある等の意見があった。これら意見を踏まえ、主査と事務局で検討し、2 つ程度の具体例アイデアを詳細化して次回議論することとなった。
- 前回指摘のあったセキュリティ研究の「科学的基礎」とは何かについて、米国の報告書等を参考にして検討された内容が委員より説明され、意見交換が行われた。提案された内容の 1 つを実現するだけで相当難しく、具体的に進めるに当たりどのように利活用・実証していくかを考える必要がある、研究がアドホックでなく再現性や客観性のあることが大切である、方法論として深めていくベースとして方向性や指針である等の意見があり、引き続き委員と

事務局で検討することとなった。

(以上、荒木委員、木村氏、須賀委員、高島氏、高橋委員、中尾参与、永山委員、本間委員、森主査、山内委員、山田委員、事務局（五十音順）

産学共同研究の具体例

- 前回以降継続して委員及び事務局で検討されてきた産学共同研究の具体例アイデア（資料 2-1）について事務局より説明され、意見交換がなされた。提案内容については成立性があるかが大切であり、堅牢化手法に係るアイデアと分析把握研究に係るものは成立性がある一方、自動運転に係るものは成立性はあるものの国の予算が前提として想定されている、認証システムに係るものはブラッシュアップが必要である等の意見があった。提案者より、堅牢化手法についてはユーザ企業と実施することも視野に入れて大学の専門性を活用できるようにされると良い、認証システムについては全体のモデル化とスコアリングができると良く利便性と安全性のバランスがとれると発展性がある等の追加説明があった。それに対し、認証システムについて、関連技術は標準化まで進んでいる一方でレガシーな慣習のために研究とは別の問題がある可能性がある等の意見があり、またシステム全体のスコアリングやリスク評価、フォーマルメソッドによるプロトコル評価、ユーザビリティへの取組に関して知見のある大学や研究会が紹介された。今後、委員から知見・意見を求めつつ事務局で更にまとめていくことになった。
- 関連して、産学共同研究は IT ベンダーよりユーザ企業の方が相手としてありえるのではないか、企業の要求に近づくほど企業からのアウトソースとしてベンダーとの競合になってしまう、企業が大学との連携に資金を出すのはリスクが大きく企業では取り組めない研究あるいは成功すると非常にリターンが大きい研究である、産学共同研究に関するユーザ企業側のメリットとして連携の波及効果やインパクトが考えられる等の意見があった。

(以上、荒木委員、鶴飼氏、須賀委員、高橋委員、森主査、八剣専門官、事務局（五十音順）

日本の強み分析のまとめ案

- 事務局より資料 3-1、資料 3-2、参考資料 1-1、参考資料 1-2 が説明された。各研究領域について、事務局によるとりまとめ素案について専門的知見を有する委員の監修を得る等して、資料 3-1 として作成された旨が説明された。その上で、意見交換がなされた。
- 研究領域の整理について、自動車セキュリティは外部ネットワークとつながるコネクテッドカーが主体であり自動運転はその出口の1つであるため事務局提案の領域名は元の領域名に戻した方が良い、手法という整理上の分類があるが手法だけではないため別の分類名を検討した方が良い等の意見があった。
- 強み分析・整理の作業結果まとめ案について、一部記述は誤解を招くおそれがあるためネガティブにならない記載に修正すべきである、センサーセキュ

リティは米国の存在感が特に大きいため現状評価は○より◎に修正すべき等の意見があった。
(以上、秋山委員、荒木委員、須賀委員、高橋委員、中尾参与、本間委員、山内委員、事務局(五十音順))

以上を踏まえ、中間報告に向けたとりまとめを事務局が進めることとなった。

(2) 中間報告に向けて

事務局から資料の説明を受けつつ意見交換が行われた。概要以下のとおり。

中間報告原案

- これまでの議論を踏まえた中間報告原案ドラフト(資料 4-1)及び重点的な研究領域の整理案(資料 3-3)について事務局より説明された。中間報告原案について、1.1 節などに現れるトーンは、これで良いと思われる等の意見があった。これを基に各委員に事務的に修正等の意見を提出してもらうこととなった。
- 重点的な研究領域の整理案に関しては、これまでの領域整理作業から導出されている整理案だが 5G やクラウドといったデジタルインフラの要素も何らかの形で考慮されるべきである、学術分野ではクラウドセキュリティは分解されて様々な研究領域で扱われていると思われる、社会的価値と経済的価値の 2 軸で表現するのは必ずしもわかりやすいわけではなく誤解を生むリスクがあるのではないか等の意見があり、次回までに委員及び事務局でメール等を通じて整理案の議論を継続することとなった。

(以上、荒木委員、中尾参与、森主査、事務局(五十音順))

以上を踏まえ、中間報告に向けたとりまとめを事務局が進めることとなった。

(3) その他

10 月下旬に開催予定の CSS (コンピュータセキュリティシンポジウム) との連携について、状況の紹介が行われた。また、今後の作業の進め方についての確認が行われた。

以上