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６回会合　議事概要

1．日時
令和２年10月12日（月）　16:30～19:00

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
（外部発表者）	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
（事務局）	山内 智生	内閣審議官
	江口 純一	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
	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）
	総務省	
	文部科学省	

経済産業省

4. 議事概要

（1）中間報告案について

中間報告案とりまとめの議論がなされた。事務局からの中間報告案の説明を受けつつ、適宜関連資料の説明も受けながら、意見交換が行われた。概要以下のとおり。

中間報告案、日本の強み分析、重点的な研究領域の整理について

- 事務局より、前回会合以降の修正として、日本の強み分析について前回会合での意見を踏まえて修正された資料 2 とその見え消し版の参考資料 2、強み分析のための研究領域の整理の修正点を示した資料 3 が説明された。また、前回会合で議論された重点的な研究領域の整理について、その後、委員及び事務局間でメール等を用いつつ議論・整理がなされた資料 4 が説明された。さらに、事務的に委員から意見が募られた中間報告案について、前回からの修正点を中心に説明がなされ、その上で、意見交換がなされた。
- 中間報告案において、シンポジウムや機械学習などいずれの専門用語を採用するのが良いか、研究構想や産学共同研究の具体例はどのように位置づけられて取り扱われるのか、本文と添付資料のスライド 1（ポイント 1 枚紙）の記載は対応させた方が良い、SecHack365 等の人材育成プログラムは研究人材を育成しているか、同様の人材育成施策である enPiT も取り上げた方が良い、研究倫理に関しては注釈の記載で良い等の議論や意見があった。
- 日本の強み分析と重点的な研究領域の整理について、14 の研究領域と重点的な研究領域の対応の説明や、デジタルインフラセキュリティの説明が不足しているのではないか、「将来を見据えて取り組むべき」などの分類の説明をした方が良い等の議論や意見があった。
- 中間報告案は適宜必要な修正を行うとともに、日本の強み分析や重点的な研究領域は説明された資料を基にとりまとめていくこととなった。

（以上、秋山委員、荒木委員、須賀委員、高橋委員、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））

研究構想の具体例について

- 事務局より、前回会合資料（資料 1-1）における通し番号 1 と 2 のアイディアの共通部分を連携させつつまとめ、分散型データ活用の具体例が、関係委員と事務局によっ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。
- 分散型データ活用の具体例について、信頼あるというタイトルとプライバシー保護の内容がずれていて関連するトラスト等が含まれていないのではないか、それに対してトラストは発展途上の研究分野であり現段階で取り入れるのが難しい、信頼あるデータは個人のプライバシーデータだけでなくまた間

違ったデータでないことも重要である、トラストに関連するブロックチェーンという用語を使用しなかったのは適用分野が広く内容が発散してしまうためである、項目Aのデータの利活用と項目Bの攻撃データの共有といった両者で異なるデータであるにも関わらず項目Cの共通技術で実現できるという点は面白い等の議論や意見があった。

- 関連して、研究コミュニティでも様々な議論が起きて新しい研究構想が出てくると良い、研究構想の具体例は WG 委員全体の納得感が重要である等の意見があった。これらの議論を踏まえ、説明された2つの具体例を基にとりまとめていくこととなった。

（以上、秋山委員、荒木委員、須賀委員、高橋委員、森主査、山田委員、事務局（五十音順））

産学共同研究構想の具体例について

- 事務局より、前回会合資料（資料 2-1）における認証システムに係るアイディアを整理・更新してサービスの安全性に関する評価手法として作成した旨が説明された。また、同じく堅牢化手法に係るアイディアと分析把握研究に係るアイディアもブラッシュアップした旨が説明された。その上で、意見交換がなされた。
- サービスの安全性に関する評価手法について、キャッシュレス決済に関連するテーマであるため実装の正しさ等も重要な観点である、実装セキュリティの関連研究として耐タンパソフトウェア、難読化、ホワイトボックス暗号方式等がある、現状フォーマルメソッドにより評価可能なのはシステム全体ではなく、限られた（制約の多い）シンプルなプロトコルへの適用に限られている、研究テーマを分割するか第一義として解決できる内容を変えた方が良い、大学と企業の共同研究として 1 対多、多対 1、多対多などどのような形態を想定しているか、1 企業が 1 つのサービスについて多くの大学と共同研究するのは経営観点から難しいのではないか、一方で対象サービスがその企業の根幹に関わるサービスであるなら経営者が多額の研究費を出すことはあり得るのではないか、（2019 年 7 月や 2020 年 9 月に）実際にキャッシュレス決済で起きた問題を想起させる例として有用である、研究が事業及び標準化やガイドラインに反映される点が好ましい等の議論や意見があった。
- これら指摘を踏まえ、サービスの安全性に関する評価手法につき事務局と関係委員で整理を行いつつ、説明された3つの具体例を基にとりまとめていくこととなった。
- 関連して、産学共同研究の具体例では成立性が重要である、対象となる研究ができるコミュニティがいるか、そのような研究できる下地があるかの情報が必要である等の意見があった。

（以上、秋山委員、荒木委員、須賀委員、高橋委員、本間委員、森主査、山田委員、事務局（五十音順））

資料 1 は、掲載する強み分析や具体例等を含め、本日の議論を踏まえて所要の修正

を行って中間報告案としてとりまとめ、研究コミュニティとの意見交換等を経て専門調査会には中間報告として報告されることとなり、最終的なとりまとめは主査一任となった。

（２）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、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（JST/CRDS）より、WG との連携を図る観点から、JST/CRDS として検討している提言である博士課程の学生支援について及びセキュリティ＆トラストの俯瞰についての発表が行われ、意見交換が行われた。

以上