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
第19回会合　議事概要

1．日時
令和4年9月29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）

（会長）	松本 勉	横浜国立大学大学院環境情報研究院　教授
（委員）	上野 裕子	三菱ＵＦＪリサーチ&コンサルティング株式会社 政策研究事業本部　経済政策部　主任研究員
	鵜飼 裕司	株式会社ＦＦＲＩセキュリティ　代表取締役社長
	小熊 寿	トヨタ自動車株式会社　コネクティッド先行開発部 ＩｎｆｏＴｅｃｈ　セキュリティグループ長
	木村 康則	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　上席フェロー
	小松 文子	長崎県立大学　教授
	寺田 真敏	株式会社日立製作所研究開発グループ システムイノベーションセンタ　主管研究員 東京電機大学　教授
	戸川 望	早稲田大学理工学術院　教授
	奈良 由美子	放送大学　教授
	森 達哉	早稲田大学理工学術院　教授

（事務局）

髙橋 憲一	内閣サイバーセキュリティセンター長
下田 隆文	内閣審議官
吉川 徹志	内閣審議官
小柳 誠二	内閣審議官
内藤 茂雄	内閣審議官
中溝 和孝	内閣参事官
佐伯 宜昭	内閣参事官
野村 至	参事官補佐
篠田 陽一	サイバーセキュリティ参与
中尾 康二	サイバーセキュリティ参与
八剱 洋一郎	情報セキュリティ指導専門官

（オブザーバー）　国家安全保障局、内閣府（科学技術・イノベーション担当）
警察庁、デジタル庁、総務省、文部科学省、経済産業省、防衛省

4. 議事概要

(1)サプライチェーン・セキュリティを中心とした研究開発の状況について
① 各省の研究開発（サプライチェーン・リスクを含む）の状況
② 経済安全保障重要技術育成プログラムにおける研究開発ビジョンについて

事務局から資料 1(非公開)、各省庁から資料 2～資料 5 の説明後、意見交換を実施。委員からの意見の概要は以下のとおり。

○ 各取組について良い成果が出ていると思う。成果やノウハウの蓄積には今後も継続的に取り組みつつ、関係者やステークホルダー間で共有する仕組みも必要ではないか。（木村委員）

○ 経済安全保障重要技術育成プログラムの説明の中でシンクタンクに言及されていたが、継続的に取り組むために、産学官が集まり、研究に取り組みながら人材育成もしていくような組織があるとエコシステムとして有用と思う。（木村委員）

○ 経済安全保障重要技術育成プログラムにおいて、サイエンティストとポリシーメーカーの橋渡し役の存在が重要と思われる。（小松委員）

○ 経済安全保障重要技術育成プログラムは社会実装を明確に射程に含め、人材育成も含まれており、エコシステム構築に寄与すると認識。特に伴走支援の仕組みに期待しており、その仕組みそのものも一つの社会技術として位置付けて、他の省庁などでも使えるように横展開できるとよい。（奈良委員）

○ 大学の先生や企業の研究者と話すと、経済安保や研究インテグリティに関して戸惑っている方が多い印象を持っている。研究開発の成果がどう使われるのか、公益的な意識を研究者にも持っていただくことが必要。（上野委員）

○ 経済安全保障重要技術育成プログラムについて、重要技術の育成、国民と国家の安全保障上の脅威への対策という側面の両方とも重要と認識している。領域として海洋や宇宙が重要技術として挙げられているところ、国家安全保障ということで軍事や防衛技術と予想する。アカデミアの立場では軍事や防衛に関する研究の敷居は高く、アカデミアの研究者を巻き込むためには、公募等工夫する必要がある。（森委員）

○ 経済安全保障関連の動きが出ているが、重要なことはサイエンスとセキュリティ、オープンとクローズに関するバランス。日本企業もかつては自前主義の傾向があったが、昨今ではオープンイノベーションが浸透しているため、国際共同研究が行われることも多く、セキュリティを確保しつつ外国と連携して技術開発していくにはどうすればいいのか考える必要がある。（上野委員）

○ 国家安全保障・経済安全保障を意識しながらサプライチェーン・セキュリティをどう実現するかについて、技術そのものと技術者を育てるという 2 点があると認識している。技術そのものを育てるコミュニティや、技術者を育てる仕組みの中の条件も一つの重要な要素と思われる。例えば、カーネギーメロン大学ではアメリカの機微な国家安全保障等に深くかかわっているスイス人の先生もいる。安全保障の観点

と相反する可能性がある一方で、そのような外国籍の技術者も人材育成対象に加え、国内産学官のサプライチェーン・セキュリティに貢献してもらうというプランについても意識していただければと思う。（小熊委員）

○ 発表されたサプライチェーンのセキュリティを担保するためのさまざまな施策・技術はいずれも重要である。これらの技術自体はいつ必要になるかをあらかじめ決めることができないが、基礎技術・応用技術を広く確保していくことが国の戦略としても重要。特に経済安全保障の観点を考えたとき、AI の活用含めた技術検証および半導体のセキュリティについての継続した研究が重要である。（戸川委員）

○ 経済産業省の発表について、IoT に関する取組はよい取組だと思う。ガイドラインの作成においては、企業への啓発に活用できるように、セキュリティ機能の設計に関するアンチパターンの事例も取り扱ってほしい。大学の立場として地域の中小企業への啓発も役割と考えており、事例があるとより伝わると考えている。（寺田委員）

○ 経済安全保障の領域において、内部不正の脅威は未だ強いと感じる。研究対象として取り組むのも一案ではないか。（小松委員）

○ 昨今の安全保障の状況を考えるとオフェンシブセキュリティに関する研究開発は、モダンな安全保障にあった防御やサイバー演習のようなトレーニングを実施するうえでも重要である。民間においても新しい市場でありビジネスチャンスも大きくなっている。一方で、表に出して取り組みにくいというのは承知している（鵜飼委員）

○ オフェンシブセキュリティに関して、個々のサイバーセキュリティ技術を高度化していくことと捉えれば研究を進めて行くことはできるが、ポリシー、ビジネス、運用といった観点と組み合わせたときに、取組の必要性などの問題が出てくると思われる。（寺田委員）

○ 安全保障でオフェンシブセキュリティは外して語れない。学者の身分でも産業の身分でも、日本でオフェンシブセキュリティが根付く気配がない。早急に何かできる状態ではないが、オフェンシブセキュリティがある程度必要と認識したうえで、政策の中に組み込めないか研究していく必要があるのではないか。（篠田参与）

以上