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 18 回会合　議事概要

1．日時
令和 4 年 2 月 22 日（火）　16:00～17:45

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
	江口 純一	内閣審議官
	山内 智生	内閣審議官
	中溝 和孝	内閣参事官
	佐伯 宜昭	内閣参事官
	小西 良太郎	参事官補佐
	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
（発表者）	盛合 志帆	国立研究開発法人情報通信研究機構 サイバーセキュリティ研究所　研究所長
	川村 信一	国立研究開発法人産業技術総合研究所 ＣＰＳＥＣ　副研究センター長

（オブザーバー）　内閣官房国家安全保障局、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）今後の研究開発課題の検討について

事務局からの資料1、有識者からの資料2及び資料3の説明を受けて、意見交換が行われた。概要は以下のとおり。

◯ハードウェアセキュリティ領域は、FPGAチップやRISC-V等を用いたデバイスのエンドユーザが拡大する中でその重要性が増している。サードパーティも含めたメーカが信頼性の高い半導体等のハードウェアを製造できるようになっていることに加えて、幅広いユーザがハードウェア設計に参画できる状況になっている。一方で、この領域は、ハードウェアそのものに対する深い知識だけでなくセキュリティに関する知識も必要になるため、研究開発への参画のハードルが高いのも事実である。

また、ハードウェアセキュリティ領域の研究振興に当たっては、経済安全保障の観点から、要素技術だけではなく、攻撃事例の収集も重要である。（戸川委員）

◯チップやハードウェアのセキュリティはもちろん重要だが、足元の脅威では、機器やソフトウェアのセキュリティ問題が深刻である。リバースエンジニアリングによるバックドア解析の取組でも、多種多様な解析ノウハウが属人的にしか蓄積しないことが課題。人的リソースの効率化やスケールメリットによるコスト低減効果の観点から、自動化を含めた解析ツールの開発や国内でのノウハウ蓄積を進めることが考えられる。

また、サプライチェーンセキュリティの観点からは、ファームウェア等のバイナリからSBOMを自動的に生成できれば、既知の脆弱性の管理がより容易になると考えられる。海外でも商用ツールがあるが、ソフトウェア構成データの漏洩などの安全保障上のリスクを踏まえ、国内でこうしたツールの開発を進めることが重要である。（鵜飼委員）

◯経営層のコミットメントを促進する観点から、セキュリティリスクや対策効果の見える化、定量化研究が重要であるが、現時点でなかなか進んでいない。警察庁公表資料においても、情報セキュリティ対策への投資に関する最大の問題として、費用対効果が見えないことが挙げられている。技術面だけではなく、幅広い分野が関わるためハードルは高いが、セキュリティ市場を拡大する観点からも取り組むべきである。

また、デジタル経済の進展に伴い、シェアリングエコノミーをはじめ社会システムが大きく変わりつつある。このような変化に応じて、中長期的に、求められるセキュリティ技術や研究開発課題にも変革が求められる。（小松委員）

◯サイバーセキュリティ分野で活用できるファンディングが潤沢に整いつつある一方で、感度が高い大学・企業やURA（リサーチアドミニストレーター）が充実した大学に留まらず、幅広い研究者がファンディングの機会を活用できる仕掛けが必要である。これは、一組織では実現が困難なことでも、データの共有など複数の組織が連携して、組織的に実施できるようにする観点からも重要。具体的には、該当するファンディングを一元的にリスト化し、テーマ、応募時期、予算規模などの概略が一覧できると、研究者がアプライする機会が増えると思う。（森委員）

◯Log4j等の脆弱性対応に際して明らかになった課題は、ハードウェア・ソフトウェア問わず、自社のシステムに何が使われているのかが分からなければ、対処がままならないという点である。例えば、研究領域として、脅威の分析だけではなく、対処の自動化に

繋がる研究や基盤整備に、産学官で取り組んでいくべきではないか。（寺田委員）

◯1 つの組織だけではなく、様々な企業・機関が持っている実データを連携させて研究や人材育成に取り組むことが肝要。加えて、1 箇所に集めるだけではなく、ネットワーク的な連携が生まれ、更に産学官で連携できることが理想である。

また、経済安全保障重要技術育成プログラムにおいても、サプライチェーンの課題は重要である。例えば、半導体のセキュリティを考える上で、流通経路でのリスクの可視化、トラスト関係の構築が課題と考えられるが、当該プログラムにおいても、新たな領域として、技術的に貢献できる可能性があると思う。（木村委員）

◯サイバーセキュリティは経済安全保障を支える基盤であり、経済安全保障重要技術育成プログラム等のファンディングの活用に向けた、研究者への情報提供が重要である。自由な公募だけに委ねるのではなく、重要な技術は NISC が一歩踏み込んでメンバーの組成や提案のサポートに取り組むべきである。

また、サイバーセキュリティ自給率が乏しい中で、最先端の技術育成ができるのか、どのような領域であればそれが可能なのか、よく検討すべきである。仮に国内シーズだけで実現が不可能であれば、海外との連携や海外技術を導入した上での開発が必要になるが、この場合には知財マネジメントが重要になる。オープンサイエンスの時代に、経済安全保障の観点から難しい舵取りが求められる。（上野委員）

◯暗号領域をはじめとして我が国でも散発的に優れた要素技術があるため、そうした技術を構成要素とするプラットフォームなど、要素技術を繋ぐ Glue（接着剤）となるような技術領域が重要ではないか。具体的には、暗号アルゴリズムとハードウェアセキュリティを繋ぐ、サービスライブラリやミドルウェアの開発などが考えられる。一方で、産業側の視点では、いかに優れた技術であっても既に提供しているサービスは止められないため、ソフトランディングできる工夫も必要である。

また、サプライチェーンに関して、情報の信頼性を高める観点から、トレーサビリティやフォレンジック技術が重要であるが、その Trustworthiness を証明する枠組みもあわせて必要となる。（小熊委員）

◯政策ニーズとして挙げられたものはいずれも重要と考えるが、我が国として自律性確保の観点から、技術の国産化やサプライチェーンのレジリエンス確保が重要である。また、ユーザ側から見れば不透明な環境下でリスクは過大に見積もられる傾向にあるため、安心という観点から、データの流通基盤の信頼性確保、トラストの可視化も重要である。

また、社会実装や PDCA サイクルを実践できる環境づくりが重要であると考えており、制度面等のボトルネックの解消や実データの提供を通じたプラクティスの提示など、国しかできないことがあれば積極的に取り組んでいただきたい。

潜在的な人材の発掘、予算の獲得双方の観点から、国民の関心を喚起することが重要であると考えている。このため、研究領域としては、実用化に近い人的要素に関わるセキュリティ領域の振興が必要だと思う。（奈良委員）

◯ファンディングのあり方として、たいていは研究開発した成果を活かしてビジネスとして自立させるような縛りが多いが、先進的な取組であればあるほど、経営層のコミット

メントを得ることが難しく、仕組みの工夫が必要。（松本会長）

◯重点領域としてデジタルインフラセキュリティが挙げられているが、クラウドサービスやゼロトラストの枠組みなど、米国発のインフラ・枠組みが先行しており、どうしても後発とならざるを得ない。実態と連動したセキュリティ研究が重要であり、自ら新しい概念のインフラを提案した上で、それに対するセキュリティ技術を研究するといったチャレンジングなアプローチが必要ではないか。

また、脅威動向が刻々と変化する中で、変動するリスクを可視化するアプローチが重要である。具体的には、動的な脅威分析や、脅威に依存する脆弱性分析、脅威に応じてポリシーを変更する仕組みなどが考えられる。（中尾参与）

◯外国企業では使用するセキュリティ製品もオープンにしている印象がある。政府として国産製品を重用したいのであれば、内緒にせず堂々と公開すればいいのではないか。

また、米国では、サイバーセキュリティに対する責任は、専門家ではなくCEOが負うべきものとされており、多くの企業ではCEOの査定でサイバーセキュリティに対する取組が評価項目とされているようだ。経済安全保障の観点からも、サイバーセキュリティに対する責任の所在を明確にすべきと考える。（八剱指導専門官）

（→米国企業では、サイバーセキュリティ対策のきっかけの約50%が経営層からの指示であるのに対し、日本は25%以下であるとの民間調査もあり、自分も普及啓発に活用している。（盛合所長））

意見交換を踏まえ、新たなファンディングの活用を含めた今後の研究開発課題の検討、取組の具体化を進めることとなった。

以　上