産業サイバーセキュリティ研究会
ワーキンググループ3(産業振興・人材育成)(第9回会合)
議事要旨

1. 日時・場所

日時:令和7年4月17日(木) 10時00分～12時00分

場所:Web開催

2. 出席者

WG3委員	:國領委員(座長)、東委員、石井委員、稲垣委員、鵜飼委員、鴨田委員、教学委員、栗原委員、篠田委員、関委員、中野委員、西尾委員、花見委員、松本委員、三輪委員
オブザーバー	:内閣官房 内閣サイバーセキュリティセンター、金融庁、警察庁、総務省、厚生労働省、防衛省、防衛装備庁、デジタル庁、独立行政法人情報処理推進機構
事務局	:経済産業省 奥家大臣官房審議官、武尾サイバーセキュリティ課長

3. 配付資料

資料1 議事次第・配付資料一覧

資料2 委員等名簿

資料3 事務局説明資料

4. 議事内容

(1) これまでの取組について

＜産業振興戦略に対する評価＞

- 国内の産業振興に向けた大きな方向性はよい。
- 戦略が具体的に示されていることを評価したい。
- ロードマップ等を通じて、大きな目標が設定されたことは評価できる。
- 今回とりまとめられた戦略は具体的なものであり、非常によい。
- 産業振興について、是非進めていただきたい。

＜取組内容への質問＞

- 資料3「先進的サイバー防御機能・分析能力強化のための研究開発」(P.15)について質問したい。国産で有益な製品を開発しているものと思料しているが、開発物の著作権や知的財産権は誰が有するのか。海外製品が普及している中で、ナショナルブランドで安心できるものでないと売れない現状がある。開発した製品の運用部分を含め、担い手について突き詰めて具体化すべきである。
- 資料3「先進的サイバー防御機能・分析能力強化のための研究開発」(P.15)について質問したい。一般社団法人「サイバーリサーチコンソーシアム」には様々な企業が参画し、連携している。人材面や技術面でセキュリティ・キャンプとの重複はないか。

  ⇒資料3に詳細を記載していないが、経済安全保障重要技術育成プログラムにおいてNICTとも連携している。また、セキュリティ・キャンプについても重複が生じないよう進めていくことを考えている。
- 資料3「サイバーセキュリティ人材の育成促進に向けた検討会議論の全体像」(P.19)では、新たなキャンプの実施について言及されているが、どのような形の実施を想定しているか。

  ⇒セキュリティ・キャンプについて資料3に記載しているが、特定の専門分野(例:AI×セキュリティ)につ

いて 50 名程度で実施することを想定している。

(2) 今後の方向性について

＜戦略の実現に向けた基盤の整備/進捗状況の把握＞

- 本戦略に不足している要素は情報基盤の整備である。戦略と戦術を結ぶために必要なものは情報であり、各ベンダーや各ユーザーが情報を活用するためには環境が必要となる。多様なセキュリティ産業事業を産業分野とするために必要な情報は、技術、人材、教育、市場、規格、国際的な法制度、資金調達を含め極めて多様で、これを収集し事業に活かす取り扱いには高い能力とコストが必要である。セキュリティ産業分野を担う事業者の、少なくとも非競争領域の情報の収集や取り扱いに資する基盤整備を国が担えば、単なる情報提供でなく情報共有を通じた産業育成のエコシステムに展開し、役立つことだろう。しかし現在は、セキュリティ事業スタートアップ企業やセキュリティ関連企業、システム開発において、この部分がアドホックで手探りのようにみえる。安全保障にもつながるテーマである。情報基盤とその情報基盤が不足しているように感じる。是非整備されたい。
- 様々な産業分野で、ソフトウェアの比率が高まる流れは止まらないと考えられる。ロードマップでは意欲的な目標を掲げていただいているが、目標に対する達成度をモニターすることが重要である。ヒト、モノ、カネ、情報の面から KPI をモニターしていく必要がある。また、状況に応じて施策を見直す柔軟性も求められる。継続的な取組を進めていただきたい。

＜セキュリティ人材の育成＞

- 国内のセキュリティ人材は不足しているため、高専や大学機関を活用していく必要がある。また、セキュリティのイノベーション制度も必要であるとの認識である。人材の集約を図り、TOB(Take Over Bid:株式公開買付)等の制度も簡略化しながら、技術開発の中心地を東京に設けては如何か。
- 高度専門人材が少ないことは事実であるため、ケアをすべきである。高等教育だけでなく、中等教育や高専での教育と連携をした上で、人材育成を進められたい。
- セキュリティ以前に、情報技術の面で日本は世界に遅れをとっている。数年前から情報系の定員を増やす大学もみられるが、20 年ほど取組が遅い。大学の研究機関を大切にすることが重要である。産業技術総合研究所ではトップ人材を採用しているものの、パイの少なさの問題がある。
- セキュリティ人材は不足しており市場価値を高く評価されているため、マスター(修士課程)からドクターコース(博士後期課程)に進学するのではなく、就職の道を選ぶ人が多い。また、現在は技術の使いこなし方に重点が置かれているが、次のセキュリティサービスを提案できるような人材を育成する必要がある。
- IPA が推進する「デジタルスキル標準」を持つ人材をどのように育成するのかにも通じるが、特にセキュリティや AI に対して研究を行うドクター人材を支援する枠組みが必要であり、全体のデザインを構築しつつ、産業化していく視点を持つことが重要である。
- 資料 3「サイバーセキュリティ人材の育成促進に向けた検討会議論の全体像」(P.19)の「施策の空白地帯」についてコメントしたい。中堅・中小企業のセキュリティ人材不足に加えて、東証プライム上場の大企業であっても、CISO を支えるセキュリティ人材の不足を感じる。例えば、攻撃も増加し、多様化している中で、人材不足のために対応できない事例が見受けられる。そもそも、セキュリティの導入計画を検討する人材さえ不足しているケースがあるため、経済産業省の施策の受け手側の環境整備も考えていくべきである。「施策の空白地帯」に「中堅・中小企業のユーザーのセキュリティ担当者など」が例示されているが、プライム上場の企業も含まれていると認識している。
- セキュリティ・キャンプの拡充や修了生コミュニティの整備は賛成である。新しいビジネスのきっかけにな

り得るため、セキュリティ人材と経営者及びグローバル企業のビジネス担当者との交流は重要である。また、今後はAIセキュリティ分野の需要が予想される。例えば、生成AIの悪用の脅威は拡大しており、対応に係る特殊なテクノロジーが必要となり、それに対応可能な人材の育成が求められる。さらに、著作権、人権に係る部分もあるため、幅広いスキルを持った人材が必要とされる。

- 資料3「今後の取組の方向性」(P.16)のなかで、仮想環境を用いた演習環境について言及されている。NICTのCYDERの取組やNISCの「普及啓発・人材育成専門調査会」での取組がみられるところ、どのような連携を行う予定か。また、「成長分野を支える情報技術人材の育成拠点の形成(enPiT)」や「サイバーセキュリティ人材育成事業（K-SEC: Kosen Security Educational Community)」等の既存の取組もみられるため、うまく連携されたい。
- 監査法人グループのコンサル機能の活用も有効と考える。会計士のリスキリングを促すことで、セキュリティ企業人材の層を厚くしていただけるとよい。
- セキュリティ人材の募集は多く需要超過であるため、セキュリティ人材自体は生活に困っていないことが多い。業界未経験でも可とする求人がある中で、需給の見直しについて議論されたい。

＜スタートアップ企業の育成/国内産業の振興＞

- 自社のセキュリティを確保するため、日本の大手企業は実績や機能の観点から海外製品を選定する。この現状を打破することは容易ではないため、10年単位の長期的な視野が必要という指摘には同意する。
- 国内のSIerは海外で実績のある製品を扱うことが多いため、国内ベンダーが商流に入れないことが多い。そうであれば、国内ベンダーが海外市場に展開することを国として後押しすることが有効である。例えば、各地で開催されるセキュリティに係る国際会議において、セキュリティ製品等の展示会にジャパンブースを設けて、意図的かつ積極的に国内ベンダーを紹介し、海外展開を促すことが逆に国内市場への参入に繋がると考えられる。
- 大企業であれば自社でツールの目利きはできるが、中堅・中小企業ではそれができない。現状では、基本的にSIer等から勧められる海外製品を導入している中堅・中小企業が多く、他方で運用サービスは日本企業に委託されている場合が多い。また、研究開発部分について中堅・中小企業への普及が課題であると考えている。
- 中小企業をターゲットとする意見には同意見である。個人的には、「サイバーセキュリティお助け隊サービス」にてこ入れができないかと考えている。SIerとしては売りやすい製品を売っていくという状況があるため、そこを切り崩すことが重要である。
- 産業振興に関する意見は他の委員と同じである。国内で強い製品が生まれるのが望ましいが、必ずしもそうならない現状があるため、国主導で攻撃情報が製品ベンダーに集約されるとよい。成熟している分野ではセキュリティスタートアップが出にくい状況であるため、新しい分野に着目すべきである。例えば、AIエージェントは新しい分野である。積極的にスタートアップを育てて、よりよい取組ができればと考える。
- 海外製品のローカライズの問題がある。海外製品が日本語に対応できていないケースがあるため、そこに速やかに対応できる企業があるとよい。
- AI スタートアップの起業家と会話する機会があったが、彼らは海外で起業をされていたため、そのような方々が日本で起業したくなる仕組みを検討されたい。
- セキュリティ特化というより、生成AIに係る要素が増えたため、セキュリティを扱うスタートアップという点においては幅広にみていく必要がある。また、Small Business Innovation Research(SBIR)の効果的な活用についても検討した方がよい。
- AI の活用に関しても、国内においては国産製品を用いるという考え方が主体になり得るのではないかとい

う議論については考えさせられるところはあった。

- 先進的サイバー防御機能の研究の一環で、耐量子暗号や耐タンパー性の研究に取り組んでいる。一方で、本取組は事業化にダイレクトに結びつかないため、ニーズのある部門と情報連携を行い、ビジネスにつなげていきたい。研究開発には時限がある点がポイントである。
- 今後はロードマップの具体化が重要であり、例えば、海外企業の成功事例や失敗事例を分析し、日本のベンチャー企業に示せるとよいのではないか。
- 20 年前から国内のセキュリティ産業振興について議論されているが、議論内容は大きく変化していない。海外企業の成功事例の分析について言及があったが、セキュリティ業界も浮き沈みが激しい。例えば、以前は政府に多く導入されていたファイア・アイの製品も現在はマイクロソフトの製品に置き換わっている。古い事例を分析したとしても、的外れになる可能性がある。ゼロトラストにおいては、マイクロソフト、グーグル、AWS がサービスの供給を占める中で、日本企業が割り込むことは難しい。
- 20 年間、同様の議論がなされているとの指摘があったが、過去の状況とは異なる期待感が個人的にはある。安全保障環境が変わったことが一番大きい。議論を進めやすい状況でもあるため、強力に進めていただきたい。デジタル庁と連携しつつ、安全保障の観点で国産化できるような仕組みができるとよい。

＜政府の金銭面での後押し＞

- 大手の SIer は、統合された大手ベンダーの製品を採用しがちである。したがって、中小企業の市場に対してエンドポイントや UTM 等の提供を促すことで、国産の会社を大きくすることがよいのではないか。セキュリティ人材が不足しているため、個別の中小企業に対して大手 SIer が対応することは難しく、補助金等を通じて、中小企業を顧客として持っている企業(例:リコーや大塚商会)を活用していくことがよいのではないか。
- 製品のサイクルが短いため、勝てる製品を早く強くすることが重要である。幅広に種まきを行い、見極めを早めることもしては如何か。官民ファンドからシーズマネーを素早く提供した上で、早く見極めるような仕掛けもあるとよい。

＜政府調達の活用＞

- 政府調達を通じて市場を作る必要がある。海外のある国の関係者と議論をすると、エンドポイントの監視ツール等については安全保障の問題から自国開発のものを用い、海外製品の使用を禁止しているようである。日本製品が海外で展開されることが必ずしも確実ではない中で、安全保障の観点から国産製品を作り、市場を形成していくべきである。国が動かなければ、市場は立ち上がらない。

(3) WG3 の総括

- 今回は、20 年間滞っていた議論を進めるチャンスである。進展しなければ、日本の経済安全保障の問題につながりかねない。各委員から切迫感を共有いただいた。
- 状況が変化していく中で、取組を進めていきたい。委員の方々には引き続きご尽力を賜りたい。

以上