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10回会合)
議事要旨

1. 日時・場所

日時:令和8年3月12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 国家サイバー統括室、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 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 (⇒部分は事務局による発言)

⑴ 供給能力強化に関する意見

- 国産セキュリティ製品は実績不足の印象や補助金制度の制約から中小企業が導入しづらく、英国事例のように無償配布・事故対応を含む支援を参考に、国産製品への補助率緩和や100%補助など踏み込んだ支援を検討すべき。(⇒中小企業支援について、デジタル化・AI導入補助金セキュリティ対策推進枠において小規模事業者向けの補助率引き上げも実施した。御意見については、今後の政策の参考とさせていただく。)
- IPAの「有望セキュリティ・スタートアップ製品・サービス等の積極的な調達実証事業」における“有効性検証”については、機能面だけでなく運用面も評価し、選定過程や調達実績の開示、国産製品の一覧化など見える化を進めるべき。(⇒調達実証事業については具体化を進める。厳密なスコアリングは難しく、ある程度定性的な評価になるが、評価結果の可視化方法を検討する。企業のセキュリティ状況の開示については、金融庁のコーポレートガバナンスコードでセキュリティ項目の追加を提案中。特に上場企業では情報発信が重要と考える。)
- スタートアップ支援は、国の政策と整合した対象の絞り込みや、試験導入を含むユーザー適合確認の強化、防衛省など中央省庁との連携が必要ではないか。(⇒スタートアップ支援は、幅広い企業が挑戦できる仕組み、またJ-Startupのように対象を絞った重点支援の双方が重要であり、連携しながら進める。ユーザーとの適合確認についても重要と認識し、防衛省とのマッチング、JNSA及びSI事業者との連携なども進めている。)
- 情報セキュリティサービス審査登録制度や新制度について、現状、登録制度は申請すれば容易に通る印象がある。事業者信頼性の確保のため、情報セキュリティサービス審査登録制度の見直しや表彰制度を創設する

べき。(⇒新制度（情報セキュリティサービス審査登録制度に 2 階部分として上乗せすることを検討している新たな制度）では事業者の信頼性確保が目的であり、サプライチェーンリスクの観点から踏み込んだ確認が必要との指摘を踏まえ検討を進める。表彰制度については今後の政策の参考とさせていただく。)

- 情報セキュリティサービス審査登録制度に、ランサムウェア対策としてバックアップ・復旧の重要性を踏まえ制度類型化の検討も必要ではないか。(⇒今後の政策の参考とさせていただく。)
- K プロ（経済安全保障重要技術育成プログラム）については、NICT(国立研究開発法人情報通信研究機構)が保有している膨大な通信観測データ活用や研究期間の継続性確保が課題とされ、施策全体の連動性を高めるための可視化・体系化が必要ではないか。(⇒御意見踏まえ今後の政策の参考とさせていただく。)
- AI が攻撃・防御の双方に使われるようになり脅威が急速に高度化する中、巨大投資が進む分野で国産技術を育てる重要性が高まっている。AI を悪用した攻撃も深まるため、この分野に挑戦するスタートアップの支援とユーザー適合性の確認が不可欠であり、防衛省の制度との連動も求められる。(⇒御意見踏まえ今後の政策の進め方の参考とさせていただく。)

⑵ 人材に関する意見

- セキュリティは投資効果の評価が難しいため、大学・企業と連携して評価手法を整備し、その結果を投資判断や産業育成に生かすべきであり、あわせて育成人数など具体的な KPI 設定も必要である。(⇒基盤強化として、高等教育機関での人材育成も重要であり、関係省庁と連携して検討したい。研究開発については継続的な支援枠組みも課題と認識している。御意見を踏まえ今後の政策の進め方の参考とさせていただく。)
- セキュリティ・キャンプの講師不足の課題に対しては、有名企業に限定せず教育事業者などへ裾野を広げるとともに、講座規模の拡大を図らなければ、政府が掲げる人材数目標の達成は難しいのではないか。特に AI に関するコンテンツの充実など、内容面での強化も求められている。(⇒セキュリティ・キャンプは今年度から規模拡大を進めており、講師確保については修了生活用など新しい仕掛けを検討している。AI 関連講義も拡充している。)
- 脆弱性発見から経営層の意思決定まで幅広い人材が不足しており、修了者の活動状況の可視化や、研修履歴の共有など、人材情報の見える化が必要ではないか。(⇒セキュリティ・キャンプ修了生の実績開示については個人情報の観点から政府・IPA による一律開示は困難だが、修了生コミュニティ内での同意に基づく可視化等、今後の政策の参考とさせていただく。)
- 中小企業では製品導入後の運用人材が不足しており、政府の支援枠組み強化とともに、登録セキスペの活用拡大、OT 領域の資格・認定制度の強化が求められる。(⇒登録セキスペについては、SCS 評価制度取得を支援する「サイバーセキュリティお助け隊サービス」等での活用を進めるなど、今後、活用機会を一層拡大していく。また、OT 領域では、IT 人材が OT を学ぶ、OT 人材がセキュリティを学ぶという双方のアプローチが必要と理解。御意見を踏まえ今後の政策の進め方の参考とさせていただく。)
- 政府・自治体・重要インフラのシステム信頼性を確保するには、高度なセキュリティ人材が不可欠であり、ICSCoE（IPA 産業サイバーセキュリティセンター）の役割は一層重要になっている。実環境で検証できる場や前段階の育成プログラムの強化に加え、データ・知識を継続的に蓄積・活用する仕組み、産業界と大学をつなぐノウハウ展開、分野横断連携も必要。(⇒信頼性確認にはインテリジェンスも求められるところ、こうした人材育成については今後の政策の参考とさせていただく。)
- 大阪・関西万博で中核人材育成プログラム修了者がセキュリティ支援に携わったことは大きな成果であり、積極的に発信していくべき。(⇒万博でのセキュリティ支援については会期中の制約があったが、今後積極的に発信していく。)

⑶ 国際に関する意見

・　我が国として、EU や米国を上回る国際水準を目指し、問題意識をもって取組を進めるべきである。経済安全保障の観点からも、セキュリティ産業の自給率向上と ASEAN などアジア地域への展開強化が必要である。
・　ASEAN ではエンドポイント製品が欧米勢の独占状態ではなく、ニーズ適合確認の仕組みや、「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」への準拠状況を開示できる仕組みが整えば、国産製品の普及が進む可能性がある。
・　米国・イスラエルで行われている大使館によるマッチングは参考になるほか、英国の小規模組織向けツールキット無償配布も有効な事例である。あわせて、ブラックハット・アジアのような国際イベントを日本に誘致することも、ビジネスマッチングの機会として有益と考える。
・　海外展開は IPA 単独では限界があり、防衛省など中央省庁の関与が望ましい。また、国内事業者による海外展開の失敗事例を官民で共有し、戦略に生かすべきである。
・　AI 関連セキュリティのスタートアップ支援も重要であり、巨大投資が進む AI 分野の国際競争環境を踏まえた政策議論が必要である。

（⇒ASEAN 展開・国際イベント誘致・メーカーと現地販売店のマッチングなど、委員の御指摘はもっともであり、外務省と連携して国際展開を強化したい。国内事業者による海外展開の失敗事例など、海外展開の課題共有についても官民で取り組みたい。）

以上