サイバーセキュリティ戦略本部
普及啓発・人材育成専門調査会
第 15 回会合　議事概要

1. 日時
令和 3 年 6 月 2 日（水）　10:15～12:00

2. 場所
Ｗｅｂ会議形式での開催

3. 出席者（敬称略）

（委員）	鎌田 敬介	一般社団法人金融ＩＳＡＣ 専務理事／ＣＴＯ 株式会社 Ａｒｍｏｒｉｓ 取締役／ＣＴＯ
	蔵本 雄一	元　合同会社 Ｗｈｉｔｅ Ｍｏｔｉｏｎ ＣＥＯ
会長	後藤 厚宏	情報セキュリティ大学院大学 学長
	下村 正洋	特定非営利活動法人日本ネットワークセキュリティ協会 幹事・事務局長 特定非営利活動法人日本セキュリティ監査協会 理事 一般社団法人セキュリティ対策推進協議会 会長
	中西 晶	明治大学 経営学部 教授
	野口 健太郎	独立行政法人国立高等専門学校機構 本部事務局 教授
	藤本 正代	情報セキュリティ大学院大学 教授 ＧＬＯＣＯＭ客員研究員
	三浦 明彦	元　全日本空輸株式会社 取締役 常務執行役員
	宮下 清	一般社団法人日本情報システム・ユーザー協会 主席研究員

（事務局）	髙橋 憲一	内閣サイバーセキュリティセンター長
	松本 裕之	内閣審議官
	山内 智生	内閣審議官
	江口 純一	内閣審議官
	吉川 徹志	内閣参事官
	上田 光幸	内閣参事官
	小西 良太郎	参事官補佐
	中野 孝一	主査
	八剱 洋一郎	情報セキュリティ指導専門官

（オブザーバー）
一般社団法人日本経済団体連合会・日本商工会議所
総務省・経済産業省・文部科学省・厚生労働省・防衛省・警察庁
内閣官房 情報通信技術総合戦略室・金融庁・内閣府（科学技術担当）

4. 議事概要

（1）“DX with Cybersecurity”の推進に向けた主な政策課題について

（2）「サイバーセキュリティ意識・行動強化プログラム」及び「サイバーセキュリティ月間」について

（3）次期サイバーセキュリティ戦略について

事務局及び各省庁から資料1～資料3-2の説明を受けて、3つの議題に関しまとめて意見交換を行った。資料1については、特段の異論はなく、会長一任の下でとりまとまることとなった。次期サイバーセキュリティ戦略の骨子等を踏まえた意見交換が行われ、委員からの意見の概要は以下のとおり。（大まかなテーマごとに整序している。）

【経営層の意識改革について】

○経営層の意識改革という言葉が出ているが、経営者にとっては、事業のどこにリスクが内在しているかを把握し、適切な対策を指示できる感性を持つことが重要である。感性を磨くために重要なのは様々な事例に触れることであり、ISACなどの情報共有の場を活用することが重要である。航空業界では「交通ISAC」という業種横断的な組織が立ち上げられているが、サプライチェーン全体では業種をまたぐことも多いため、業種を問わない情報共有が重要であり、各種事例集の作成や経済産業省の「SC3」の取組においては、縦割りとならず横串をさすよう取り組んでいただきたい。これと並んでインセンティブ付けも重要であり、「デジタルガバナンス・コード」やそれに基づく「DX企業認定制度」についても、ぜひ普及に取り組んでいただきたい。（三浦委員）

○「コーポレートガバナンス・コード」の改定で、取締役の知識・経験・能力等を一覧化したいわゆる「スキル・マトリックス」の開示が求められることとなり注目されているが、この中でサイバーセキュリティに関する知識の重要性についての啓蒙に取り組んではどうか。（中西委員）

【地域における取組について】

○セキュリティ人材の「学」の側からの輩出に向けて、例えば、若年層へのアプローチという観点からの文部科学省の協力や、警察庁をハブとした各都道府県警との繋がり、経済産業省が進めている「地域SECUNITY」の取組や高専と産業界との連携など、様々な行政機関がうまく連携することが重要である。また、最近では、地元の金融系企業からの人材面での関心も高く、こうしたプレーヤーの参画を後押ししていくことも重要である。（野口委員）

○地域での連携に当たっては、地域ごとのミクロの連携だけではなく、コラボレーション・プラットフォームといった日本全体のマクロの連携も重要である。そのためには、高専、大学といった単位で窓口を一本化することが望ましい。（野口委員）

○資料3-2 p.22（総務省③）において「IoTセキュリティ人材」という用語があるが、小中高の教育内容などを含め、育てる人材像が戦略においてブレてしまうのはよくないので留意すべき。（野口委員）

【サプライチェーンリスクへの対処について】

○中小企業におけるサイバーセキュリティリスクは、①企業自身に与える影響と、②サプライチェーン全体に与える影響と2種類あると考えるところ、①への対策は進展している一方で、②への対策に向けては更なる工夫や①への対策との連携が必要。例えば、サプライチェーンを構築する側から、「お助け隊サービス」の利用や「SECURITY ACTION」の取得について働きかけを行うことが有用と考えられ、こうした取組を促す分野ごとのガイドラインのようなものが示されると、更に取組が推進されるのではないか。（八剱指導専門官）

○サプライチェーンリスクへの対処について、対応コストを誰が負担するかという議論に向き合う必要がある。業種・業態によっても求められる対策が異なる中で、共同セキュリティセンターを作って中小企業の負担を減らすことも考えられる。（下村委員）

【「プラス・セキュリティ」知識の補充について】

○コロナ禍に対応して作られたシステムに様々な不具合が出ているなど、企画・設計段階で機能要件にセキュリティが組み込まれていないことが問題となっている。こうしたシステムの企画・設計の担当者に必要な専門知識も含め、「プラス・セキュリティ」知識を補充することが重要である。（宮下委員）

○学生や研究者から「プラス・セキュリティ」に対する関心が増えてきており、キーワードを作って普及啓発を行うことの重要性を感じている。教育者としてプログラムの試行錯誤を続けているが、理想論だけではなく、規模や業種、ニーズによって内容や形式の変更を行うなど、現状に即したプログラムづくりが重要であると考えている。例えば、セキュリティ対策を実施するために具体的にどのような方法をとるべきか教えてほしいというニーズもあり、実践的な知識も含めたプログラムも必要になると思う。（藤本委員）

○「プラス・セキュリティ」の重要性が共通認識になった。今後、いかに具体化していくかが重要である。ユーザのニーズに対応する観点から、IPAをはじめ官民横断的に教育プログラムを開発すべきである。また、企業内の階層別研修で取り上げられることが非常に重要。しかし、現在は、法務や会計等が中心で、DXやセキュリティの研修の場がない。階層別研修等に活用できる教材の体系的なプログラムづくりも期待したい。（三浦委員）

○官民でのガイドラインやセミナーの供給は進んでいる一方で、会社で勉強する雰囲気ではない、文書を読んでも理解できない、ガイドラインなどのドキュメントがどこにあるかわからない、といった課題も聞いており、ボトム層へのアプローチを検討する必要がある。具体的には、セキュリティ以前のIT知識の基礎教育や経験が蓄積される人事施策、教える側の質の向上といった取組が必要と考える。（鎌田委員）

【人材流動・マッチングの促進について】

○官民での人材交流を更に推進すべき。ただし、そもそも日本ではジョブ・ディスクリプションを明確化する文化が根付いていないところ、根本的な取組もあわせて必要ではないか。（下村委員）

○JUAS として経済産業省に協力する形で、プラクティス集や Tips 集の作成に取り組んでいるが、体制構築以上に、人材育成・確保に関するプラクティスを収集することは、企業の人事施策にかかわる内容のため難しさがある。一方で、セキュリティ対策の推進に向けて人事担当者や経営企画の担当者の協力は不可欠であり、具体的にどのようにセキュリティ人材を確保するか、人事制度にどのように反映させるか、それら担当者が参照できるプラクティスの共有は非常に有用だと思う。(宮下委員)

【体制構築、実務者層・技術者層の育成について】

○この数ヶ月でサイバー攻撃によって得られた情報の交換、特に日本に関する情報が増えてきている印象があり、脅威が高まっていると認識している。一方で、実際にサイバー攻撃を受けた企業に聞くと、その原因は古典的なものがほとんどであり、新しい防御方法を取り入れるのではなく、全方位防御を徹底することが重要である。セキュリティ対策の担当者は、教科書的内容だけではなく、より実践的な内容を学ぶ必要がある。(鎌田委員)

○取組が進展している自動車産業においては、セキュリティ担当者に求められる素養として、①英語力、②法規制に関する知識の重要性が増している。特に前者については、サプライチェーンのグローバル化が進む中でサプライチェーン管理上必須であり、もはや英語力がなければプロジェクトにアサインされない状況。(蔵本委員)

【その他(研究開発・情報共有・普及啓発について)】

○研究開発における国際競争力の強化を更に推進していただきたい。通信プロトコルや OS は海外に席巻されているが、国家安全保障の観点からも、そういった基礎技術の種火を消さないことが重要である。セキュリティはセンシティブな研究領域であり、研究者が安心して研究できる環境づくりも重要である。(下村委員)

○資料 3-2 p.3 (NISC②) において被害事例の収集を行うとあるが、これまでは被害事例の情報共有に抵抗感のある事業者が多かった。JUAS においても、情報セキュリティ WG で対策の横展開に取り組んでいるが、会社ごとに情報共有の仕組みが異なり、組織をまたいでセキュアに情報共有することの難しさを感じている。国から、何らか信頼できる情報共有の仕組み・サービスを推奨してもらえると、社内での承認がとりやすくなると思う。(宮下委員)

○コロナ禍でのテレワークの増加などへの対応としては、産学官の取組だけではなく、家庭における取組も重要である。高齢者を含め、セキュリティ知識が届きにくい方々への啓発にもあわせて取り組む必要がある。(中西委員)

以上