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 14 回会合　議事概要

1. 日時
令和 3 年 1 月 21 日（木）　15:00～17:00

2. 場所
Ｗｅｂ会議形式での開催

3. 出席者（敬称略）

（会長）	後藤 厚宏	情報セキュリティ大学院大学 学長
（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	合同会社 Ｗｈｉｔｅ Ｍｏｔｉｏｎ ＣＥＯ
	志済 聡子	中外製薬株式会社 執行役員 デジタル・ＩＴ統轄部門長
	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 教育参事 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	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 参与
（事務局）	髙橋 憲一	内閣サイバーセキュリティセンター長
	山内 智生	内閣審議官
	松本 裕之	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
	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）		
	桐山 篤之	一般社団法人日本経済団体連合会 産業技術本部

梶浦 敏範	一般社団法人日本サイバーセキュリティ・イノベーション委員会 代表理事
村上 晃	一般社団法人日本シーサート協議会 理事長
荒金 陽介	産業横断サイバーセキュリティ人材育成検討会 副会長
秋元 学	日本商工会議所 情報化推進部 主査
木内 直人	独立行政法人情報処理推進機構 産業サイバーセキュリティセンター 企画部

他関係団体・企業
総務省・経済産業省・文部科学省
内閣官房 情報通信技術総合戦略室・金融庁・防衛省・警察庁

4. 議事概要

（1）”DX with Cybersecurity”の推進に向けた主な政策課題の検討状況について

事務局及び藤本委員から資料 1-1～資料 1-7 の説明を受けて、委員からの意見の概要は以下のとおり。

【政策課題①：サイバーセキュリティ確保のための新たな開発・監視・対処体制の構築】

○消費者からみれば、不具合が発生した際に、それが品質の問題なのか、セキュリティの問題なのかわからない。自動車業界でみられるように、今後、セキュリティ機能は品質管理機能と一体となっていくのではないか。また、セキュリティも品質の問題であるという考え方は、経営層にとって身近な課題として訴求しやすいのではないか。（蔵本委員）

○DSIRT/SSIRT に今後求められる対応の特徴として、①開発のスピード感が早くリリース・スケジュール優先の傾向があること、②対処する人材には知識以上に実践的な経験が重要となること、③脆弱性への対応に国内外の様々な企業が苦戦しているが、迅速な対応が求められること、が挙げられる。会社全体を見渡してスピード感とセキュリティのバランスをとることが重要であり、CISO が経営側の視点でリーダーシップを発揮することが求められる。（鎌田委員）

→CISO に更なる役割が期待されるということだと思うが、国内で CISO の役割についてどのような議論が行われているか。海外もすべてがうまくいっているわけではなく、CISO がそれぞれ悩みを抱えているようである。（後藤会長）

→CISO の状況をみると社内で立場が強くなく、リリース直前にセキュリティ部門への相談が行われるケースや、リリースが優先されて事後的にセキュリティ問題が発生するケースもみられる。また、CIO と兼務のケースが多く、どちらかというと事業推進に軸足がおかれているケースもみられる。少ないとは思うが、事業推進とセキュリティの両方を考えられる立場の人が調整役になるとよい。（鎌田委員）

○CSIRT が事後対応重視の傾向がある一方で、DSIRT/SSIRT のように、企画・開発段階からセキュリティを落とし込む機能は重要。しかし、そうした機能を担える人材が少ないことが課題であり、こうした人材を育成する観点からも「プラス・セキュリティ」

知識の補充は重要。（三浦委員）

○xSIRT に関する分析は重要であるが、名称だけが先行し、それぞれの組織を別個に作るべき、といった伝わり方にならないよう注意が必要。様々なあり方が存在するため、機能するようにすべき。（中西委員）

○サプライチェーン又は製品ライフサイクルの中で、製造現場とセキュリティの情報共有も重要だが、製品の利用者側の企業の CSIRT からの声が製造企業の PSIRT と情報共有され反映される仕組みも重要ではないか。（後藤会長）
→金融業界では、リテラシーのあるユーザーから見ればこんな認証しかしていないのか、と明らかにわかるものがリリース後に判明するケースもみられ、ユーザー視点の意見は十分に拾われておらず、ユーザー視点からのセキュリティが開発時にも必要であると思う。（鎌田委員）

【政策課題②：DX に必要な「プラス・セキュリティ」知識を補充できる環境・人材育成の推進】

○「プラス・セキュリティ」知識の体系化は、セキュリティが経営リスクであるという認識の薄いグループ会社の経営陣にとっても、事業部門・経営企画部門のマネジメント層にとっても必要性を感じる。特に、基礎知識も重要だが、経営層はセキュリティの専門家でなくてよく、どんなところにリスクがあるか、という感性・感覚を養うことが重要であり、プログラムではもっとケーススタディを増やすとよい。また、その観点で、政策課題１で挙げられた事例集を作成する取組は推進されるべき。（三浦委員）

○「学」に求められる役割として、ピラミッドの下から「プラス・セキュリティ」知識を備えた人材を育成して社会人として送り出すことも重要。そのためにも、「産」の側において、そうした人材ニーズが採用の現場に反映される仕掛けが必要。（野口委員）

○私立文系大学においてもデータサイエンスも含めた IT 基礎知識を教えるプログラムが増えてきており、DX 人材育成の中で、セキュリティもそのコンテンツの１つとして位置づけられるとよい。また、大学では社会人のリカレント教育を担う機能も考えられる。（中西委員）

○JUAS が実施するヒアリングの中でも、「プラス・セキュリティ」知識に対する考え方は明確ではない。対象として、①セキュリティ統括業務、②事業部門、③PSIRT 又は DSIRT/SSIRT に従事する人材が考えられるが、それぞれに必要な知識が異なるため、体系立てて切り分けた方がよい。（宮下委員）

○現状、DX を進める場合に怖いのはセキュリティである。組織内でも CSIRT に閉じない全社的な取組となるよう体制を立ち上げており、「プラス・セキュリティ」知識の提供が必要になっている。藤本委員実施のプログラムにも、アプリ開発に携わる人材を受講させたところだが、今後のこうしたプログラムの展開に期待しており、IT だけでなく他の部門からも積極的に組織内の人材を参加させたい。（志済委員）

【政策課題③：サイバーセキュリティ人材の活躍の促進に向けた流動性とマッチングの機会の促進】

○組織内で人材募集を行うと一定の流動性があると感じている。他のユーザー企業の経験者が多く、転職を自らのスキルアップと捉えているようである。一方で、組織にマッチする人材を採用するためには、明確なジョブディスクリプションを作成することも重要である。（志済委員）

○デジタル庁の動向はデジタル化の象徴的な動き。民間、官、自治体における人材のいわば「テストベッド」あるいは「道場」として活用されていくモデルが創出されることを期待。（志済委員）

○企業、個人、教育機関に加えて、「官」もセキュリティ人材が経験を積む場所として重要である。それぞれのプレーヤーがどういう役割を果たすのかを考えながら政策を検討すべき。（下村委員）

○副業・兼業の促進に向けては、組織から人材が出ていくことをロスであるとして、流動化をマイナスイメージに思いがちであるが、経営的にはよい人材が入りやすくなるための手段と捉えて意識改革を図るべき。また、個人に対しては自らのスキルアップにつながる支援が必要である。（下村委員）

○地方・中小企業にもフォーカスを当て、空間的な軸を立てて分析をしていただきたい。その中で出てくる課題として、①地方と都市をどのように結びつけるかについては人材紹介事業者の役割が重要になるであろうし、②いかにコミュニティ形成を図るかについては、総務省や経産省で進めている取組との連携が期待され、学と地域のつながりにより人材を輩出するという好循環が起きるとよい。（野口委員）

○産学で人材の循環が生まれることも期待される。例えば、今年大学に入学した学生が卒業してユーザー企業に入社するときに、必要な知識を得られるようになっているといった形が考えられる。（中西委員）

○CISSP 等の資格を有していても、セキュリティ担当にアサインされていないケースも多く、組織内での人材の登用・マッチングの問題もみられる。（宮下委員）

（２）今後の検討の方向性について

事務局から資料２の説明を受けて、委員からの意見の概要は以下のとおり。

【経営層の意識に関する意見】

○JUAS が実施している IT 企業調査の本年度調査（1/19 に速報公表。以下同じ）では、新型コロナ影響もあり経営層の関与度合いが４割程度まで上がっている。セキュリティリスクについて経営会議で審議・決定される割合は、売上高１兆円以上では９割程度だが、売上高 100 億円未満の企業では３割程度であり、インシデント時のみセキュリティの議論がなされるなど、企業規模によって大きな差異がみられる。（宮下委

員）

○CISO が経営会議に参画している割合は大きくないのではないか。その原因として、最近はサイバー攻撃を受けても株価に大きな影響がないことや、発生した損失が特別損失計上され、多くの経営者が経営指標とする経常損益に反映されないことも挙げられる。CISO が経営会議に参画できるようにするステップも大事。また、海外の機関投資家の参入も増えている中で、中長期的には有価証券報告書への記載事項に関する要求事項を変更していくことも考えられる。（蔵本委員）

○経営層への訴求には、ホラーストーリーだけではなく、企業価値向上につながるという説明も必要。ダウジョーンズが示す「サステナビリティ・インデックス」においてもセキュリティに関する項目が増えた。経済産業省が策定した「デジタル・ガバナンス・コード」においても、望ましい取組例として、「経営者がサイバーセキュリティリスクを経営リスクの１つとして認識し、CISO 等の責任者を任命するなど管理体制を構築する」ことが定められており、組織内でも経営会議で誰を任命するかといった具体的な議論も行われている。こうした意識は DX を進める中で経営層が持つべきであるとともに、ステークホルダーに示すことも必要であり、今後その動きは広がっていくと思う。（志済委員）

○経営層のアウェアネスを高めるためには、ほめていくアプローチも必要。公開してよいことがないと経営者もやりがいがないと思う。IT 団体連盟で実施している調査において、第３者の評価に基づく業種別のランキングや好事例の紹介を行っている。「サイバーセキュリティ月間」とあわせて、何らかのアワードを出すことも考えられる。（下村委員）

○経営層に対しては、DX とセットで訴求していく必要がある。今回藤本委員の下で実施されたプログラムでも、前提知識がないという条件のハードルが高かった。その観点からも、経営層への啓蒙が重要。（八剱指導専門官）

【人材の不足感に関する意見】

○JUAS が実施している IT 企業調査の本年度調査では、人材種別でみると、実務担当者の不足感が 65％と最も大きい。一方で、スペシャリストが必要な領域はベンダー企業に入ってもらうことが一般的だが、今後は脆弱性対応など内製化も求められる中で、セキュリティ対応を全社的にリードし社内調整を進められる人材が必要になる。（宮下委員）

○金融業界では部分的にではあるが、現場の技術者は足りてきつつあるという実感がある。エキスパートも金融 ISAC を通じて業界全体に貢献しており、一時よりも進んでいると感じている。メガバンクではむしろ、知見を有する経営層や戦略マネジメント層が不足していて、戦略マネジメント層がいてもセキュリティを理解してくれないという話を聞く。地域金融機関の中でも、優秀なところがある。（鎌田委員）

○トップガンの知見が求められる場面では外部サービスを受けることが通常であり、各組織でそういった高度な人材までは不要であり人材は足りていると思うが、技術情報

を社内で説明し説得できる人材は、事業への理解も必要であり不足している。（下村委員）

【その他の意見】

○ダイバーシティに関して、女性活躍だけではなく、例えば発達障害の方など多様な方がセキュリティで能力を発揮されている。様々な形のセキュリティ人材を考えるべき。（中西委員）

○米国において、地域の CISSP の資格保有者などのセキュリティ専門家人材が情報交換を行うコミュニティがあり、仕事のポジションに関する情報も交換されていたりする。日本では、人事制度によるところも大きいが、セキュリティ人材の中でも、「プラス・セキュリティ」人材が多いのではないかと思う。わが国のセキュリティ人材について、実際にはどのようになっているかを改めて把握することも大切なのではないか。（藤本委員）

○JUAS が実施している IT 企業調査の本年度調査では、新型コロナ影響もあり企業内での IT やセキュリティ関連予算は大きく増加している。ただしその多くはテレワーク等の対応に向けられているようである。ゼロトラストのような次のステップに進んでいけるのかが課題である。導入している企業は少ないが、約 4 割の企業が検討を始めている。（宮下委員）

（3）サイバーセキュリティ月間について

事務局より、資料 3 の説明を行った。

以上