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 18 回会合　議事概要

1．日時
令和 4 年 9 月 1 日（木）　10:00～12:00

2．場所
Web 会議形式での開催

3．出席者（敬称略）

	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	日本アイ・ビー・エム株式会社 セキュリティ事業本部
		コンサルティング＆システム・インテグレーション パートナー
（会長）	後藤 厚宏	情報セキュリティ大学院大学　学長
	志済 聡子	中外製薬株式会社 上席執行役員
		デジタルトランスフォーメーションユニット長
	島　 健夫	一般社団法人日本情報システム・ユーザー協会 参与
	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	ANA ホールディングス株式会社 常勤監査役

（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
小柳 誠二	内閣審議官
上村 昌博	内閣審議官
内藤 茂雄	内閣審議官
中溝 和孝	内閣参事官
山田 剛士	内閣参事官
佐伯 宜昭	内閣参事官
野村 至	参事官補佐
篠田 陽一	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）

内閣官房（こども家庭庁設置準備室）・内閣府・警察庁・金融庁・総務省・
文部科学省・厚生労働省・経済産業省・防衛省・
情報処理推進機構（IPA）・日本経済団体連合会・日本商工会議所

4．議事概要

（1）「サイバーセキュリティ意識・行動強化プログラム」の見直しについて

事務局より資料 1-1（非公表）および資料 1-2（非公表）の説明を行い、意見交換を実施。委員からの意見の概要は以下のとおり。

○ 直近の脅威動向について、フィッシングメールのターゲット（ここではフィッシングの名称等を騙られてしまう組織）が拡大しており、従来の大手銀行に加え、保険・証券や地方の中小金融機関を騙るものも観測されている。シニア層や子ども層と話すと「よくわからないが怖いので気にする」ぐらいの認識。ポスター、テレビ、YouTube 等、様々な媒体が活用されている中、どの世代にどの媒体での発信が正しい理解に結び付いたのかを調査し、効果的な情報発信方法を検討するのも一案。（鎌田委員）

○ 認知度の向上が全ての層で課題として出ている。サイバーセキュリティに興味ない人への工夫も必要。（蔵本委員）

○ ある程度サイバーセキュリティついて知っている人も一昔前の知識で大丈夫と考えているケースもある。そういった時間軸の観点で普及啓発を今後どう展開するかも重要。（後藤会長）

○ SNS で画像をアップロードして、個人情報が抜かれる話がある。このような事例も交えつつ、こどもの被害事例について近親者が注意できるよう、工夫が必要ではないか。企業向けの話であるが、大企業のグループや関連する中小企業はまだサイバーセキュリティに関するガイドライン等を意識する機会があるが、特にサプライチェーンに入らないまたは意識することがないような中小企業は、それらに触れたり、取り組むことがなく、寄り添うような施策が必要ではないか。（志済委員）

○ 中小企業への対策としては、一人情シスへのコンテンツやツール提供が重要で、それらは充実してきてはいる。ただ、一人情シス状態の中小企業の担当者がコンテンツやツールを知った時、いざ自社に取り入れようとする際に持って行く時に考え込んでしまうことがある。「サイバーセキュリティお助け隊」のようなところで、これらコンテンツやツールの紹介や導入サポートがあるとよいのではないか。IPA 作成の「中小企業の情報セキュリティ対策ガイドライン」の自己診断ツールの結果などとあわせて使うとさらに有効になうように思う。（島委員）

○ 相談窓口の可視化は大切だが、ユーザーがそこにたどり着けるかが課題。高齢者は近親者に相談する。そのようなファーストコンタクト対象にセキュリティ等を教えることが重要。全般的なリテラシーを教えつつ、昨今増加している詐欺等の具体例について教えておくことが必要。一般の方がセキュリティ事故にあうのは、詐欺が多い。

JNSA を騙る詐欺も続いている。詐欺やフィッシング等の対策組織やサイバーセキュリティ関連組織が共同で啓発できればよいのではないか。（下村委員）

○ 学生は地域よりもネットコミュニティの影響を受けやすく、インフルエンサーから情報を得ていることが多いように思う。そのような方から情報発信いただくことも効果的ではないか。メガプラットフォーマーを想定した啓発も重要。（中西委員）

○ 今後の方向性はよく纏まっており、多様な対象へのリーチが可能となるだろう。現場は様々なところから多くのことをやれと言われて混乱している。優先順位付けが必要。DX 推進の一環としてサイバーセキュリティがあるように見せることも重要。（野口委員）

○ 「セキュリティに関する気づきを与えるコンテンツ」と「知識をインプットする機会に参加する動機」が重要。例えば、シニア層に対しては、新聞や TV といったメディアを活用した情報発信なども有効と思われる。参加を促す周知について工夫が重要。（藤本委員）

○ サプライチェーンの中で中小企業が例として挙げられているが、それら企業が経営リスクとしてサイバーを認識することが重要。まずはガイドラインやツールの認知度を挙げていくことが重要。その上でインセンティブ等の制度設計が必要ではないか。業界内の情報共有は進んでいるが、業界をまたがる情報共有も重要。航空の世界では、通信インフラ、エンジンなどの統合したセキュリティ確保が必要だが、これらの情報共有は不十分。人流を促進するような施策も必要。（三浦委員）

○ 情報モラル教育が進めば、児童・生徒が家庭のリテラシーをリードするようなことにつながり、さらに日本全体のリテラシー強化につながるのではないか。また、日本において警察の信頼感は高く、彼らによるサイバーセキュリティの普及啓発も有効ではないか。（八剱専門官）

（2）経済産業省におけるサイバーセキュリティ等の人材育成の取組状況について

経済産業省より資料 2 の説明を行い、意見交換を実施。委員からの意見の概要は以下のとおり。

○ 私立文系大学の学生には、ビジネス系の学部であっても IT や DX が若干遠いという学生もいる。今後社会に出て行く、非 IT 分野出身の一般学生が最低限身に付けておくべきスキルとは何か等、学生が自ら主体的に取り組む動機付けも必要ではないか。（中西委員）

○ DX 推進人材に必要な専門的なデジタル知識・能力が 5 つに分類されている。このうちサイバーセキュリティスペシャリストの定義に「IT システムをサイバー攻撃の脅威から守る」と記載されているが、守るべき対象は IT に限定されないのではないか。DX 推進におけるリスクとは、サイバー脅威を含めた事業リスク全般、データの管理等、DX 推進の過程で想定されるあらゆるリスクが含まれ、これらの洗出しや対

策の検討は、本来全体設計を行うアーキテクトの仕事でもある。この点がミスリードされないようにした方がよいのではないか。（下村委員）

○ p.2 の DX の成功パターンのプロセス図は、「DX の取組を通じて何を実現するのか」が決定していることが前提になっているように思う。AI 隆盛の時に見られたように、多くの DX 案件では、「うちも DX で何かできないのか？」という曖昧なトップダウンをきっかけとして「DX で何を実現するのか」という意思決定をしないまま走り出し、結局何の成果も出ないというケースが散見されている。本来はこのひとつ前に、最も重要な「デジタル技術を活用して、どのようなビジネスを展開するのか」、「そのためにどんなステークホルダーを巻き込む必要があるのか」という、デザインのプロセスと、それを担う能力を有するプラス DX 人材が必要ではないか。（蔵本委員）

○ DX 人材について体系的に整理されていると思う。DX 人材にまず必要なのは「変革のためのマインドセット」であり、そのうえで更に「専門的なデジタル知識」という強みを付加していくという定義には共感できる。これまで、DX 推進にはサイバーセキュリティの同時推進が不可欠として、「DX with Cybersecurity」を標榜してきた。そうであれば、デジタル人材育成プラットフォームの 1 層から 3 層にも、セキュリティの要素を組み入れるとよいのではないか。（三浦委員）

○ プラス・セキュリティ知識の普及促進の過程においては、「認定プログラム」のような仕組みがあるとよい。この認定を受けることで、学生の就職活動においてプラス評価がなされるような仕組みがあれば、主体的に取り組む学生が増え、学校側のプログラム提供意欲にもつながるのではないか。こういった仕掛けがないと、継続的に優秀な素養を備えた人材を育成していくことは難しい。（野口委員）

○ 実際の DX 推進の現場では、p.2 で示されるようにスムーズに左から右に進んでいくわけではなく、多くはプロセス 2 と 3 の間で何度も試行錯誤し、無事に 2 の過程を生き残った案件だけが 3 の本格推進に進めるという非常に厳しい現実がある。そのため、DX 推進の取組は従来の成功前提で開始する案件とは異なり、失敗ありきであること、それゆえに推進を取りやめる条件の設定も重要ではないか。p.3 の人材像は、企業にとってはプロジェクト編成の参考になるため有効であるが、今後も変わりうるものと思われる。（島委員）

○ デジタル人材育成プラットフォームは、サイバーセキュリティと一体的に推進していく必要がある。学校や地方自治体では、DX 推進の取組が遅延している印象があるため、そういった組織にもこのプラットフォームを活用してもらいたい。また、情報処理安全確保支援士の魅力や優位性がしっかりと伝えることも必要。この資格を保有するメリットをアピールする機会や仕組みを整えることも、セキュリティ人材の育成・増強に有益ではないか。（志済委員）

○ ここ数年プラス・セキュリティ人材の育成に取り組んでいるが、実際に育成講座に参加するのは、既にセキュリティ業務に従事している人が多く、なかなか「プラス・セキュリティ知識の補充」という点で手ごたえを感じられないでいる。DX を推進している方等の本来の対象に関心を持ってもらい、ポイントを押さえたコンテンツを提供するためにも、「その人たちが求めている知識とはなにか」を把握する取組も重要だと思う。（藤本委員）

○ ユーザーサイドの大企業を前提とすると、DX 推進の担当者や、IT 部門におけるシステム開発の担当者は、セキュリティは「セキュリティ担当者がやるべきこと」という意識がまだまだ強いと感じる。そういった人たちも、セキュリティについて学ぶ機会があれば学んでみたいと思っているものの、実際は目の前の業務が多忙で時間がない、上司の許可・理解を得られずに着手できないという現状がある。（鎌田委員）

○ 日本では、まだまだ IT 部門の担当者がセキュリティを含め何でもやらされている状況が多い。大手金融機関について日米比較すると、米国におけるセキュリティ担当組織は IT 部門から独立しており、かつセキュリティ組織内での業務分掌もより細分化されている傾向が強い。（鎌田委員）

○ このような組織構成や内部での役割分担の在り方等についても、今後どうすべきかを議論する必要がある。（鎌田委員）

○ 直近のランサムウェア被害による混乱を見るにつけ、サプライチェーンのレジリエンスが不足していたことが明らかになった。今後 DX でもサイバー脅威の顕在化が問題になるであろうし、このリスクを見分ける人材も必要ではないか。（後藤会長）

（3）総務省におけるデジタル活用支援推進事業について（報告）

総務省から資料 3 の説明を行った。（意見交換の時間は設けなかった。）

（4）サイバーセキュリティ関係法令 Q&A ハンドブックの改訂について（報告）

事務局から資料 4 の説明を行った。（意見交換の時間は設けなかった。）

以上