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 17 回会合　議事概要

1．日時
令和 4 年 6 月 10 日（金）　16:00～17:45

2．場所
Web 会議形式での開催

3．出席者（敬称略）

（委員）	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
	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

※鎌田委員、志済委員は欠席。事前にうかがった意見を事務局より読み上げ。

（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
	山内 智生	内閣審議官
	江口 純一	内閣審議官
	中溝 和孝	内閣参事官
	佐伯 宜昭	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）
内閣府（科学技術担当）・金融庁・デジタル庁・総務省・
文部科学省・厚生労働省・経済産業省・防衛省
CRIC-CSF・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

事務局から資料 1-1 および資料 1-2 の説明を受けて、意見交換を行った。委員からの意見の概要は以下のとおり。

○シニア層向けの対策として、マイナポータルなどの行政手続を利用開始するタイミングにあわせて、セキュリティもチェックリスト的に意識できるようにすべきではないか。デジタル庁と NISC、各府省の同期の取れた取組に期待したい。（志済委員）

○web だけではなく対面や電話等で相談対応できる仕掛けが必要。（志済委員）

○近年大手メディアもサイバーセキュリティに関する脅威を報じるようになってきている。通常の報道の範囲も含めて、マスメディアとコラボレーションした政策発信が重要ではないか。（鎌田委員）

○最近は動画サイト等を通じた無料 DL によるマルウェア感染が多い。9 か条のどこかで「出元のしっかりしたものを使う」という趣旨を入れるべきではないか。（鎌田委員）

○地域のセキュリティコミュニティのとりまとめ役として地域金融機関に期待する声があるが、人事の入れ替わりが激しいことが課題。中小担当者向けに特化した研修コンテンツの充実や取組事例の共有、コミュニティ形成が重要。また、地方の地場の IT 企業、支社の実力が乏しく底上げが必要ではないか。（鎌田委員）

○シニア層向けの対応として、マスメディア、特にテレビやラジオの活用が有効ではないか。（下村委員）

○中小企業向けの施策として、防災管理者と同様にサイバーセキュリティ管理者の設置を義務付け、定期的に研修を受けさせてはどうか。責任やコミュニケーション・パスが明確化され、経営層にもプレッシャーになると思う。（下村委員）

○対面でのサポートが重要。SPREAD のような枠組みを全国展開しデジタル推進委員と同様の仕組みとするか、デジタル推進委員の領域拡大をしてはどうか。（下村委員）

○認知機能の問題に関連したユニバーサルなケアの提供や、訪日外国人向けの多言語対応などは、後回しになりがちなので念頭に置く必要がある。（三浦委員）

○サプライチェーン管理上サイバーセキュリティが重視されていく一方で、多くの中小企業では人材やセキュリティ投資の余力が不足しているのが実情。対策実施に対する強制力やインセンティブの付与について検討が必要ではないか。（三浦委員）

○IT 機器だけではなく IoT 機器についても利用上注意してもらう必要がある。啓発機会の観点から IoT 機器の販売員の意識醸成なども考えると良いのではないか。（藤本委員）

○9 か条に「パスワードは長く複雑に」とあるが、一部では、記号が使えないなど安全性レベルが低くなるような設定が行われている。ユーザーだけではなく、サービス提供者への啓蒙も必要ではないか。（蔵本委員）

○中小企業で多い「一人情シス」の方に対して、対策実施をしてもらう仕掛けが必要。

「一人情シス」担当者は、社内外に相談相手がおらず、「何から手を付けて良いかわからない」状態だと推測されるため、自社のセキュリティレベルに関する自己診断シートの提供や、最近の脅威等のトレンドに関する発信が有効ではないか。（島委員）

○産官は人材の流動が多く継続が難しい一方、学は産官と比べて人材の流動が少ないため、地域のコミュニティの中心となり得ると思う。学側に対するメリットを示すことができれば、継続的な仕組みになるのではないか。（野口委員）

○各重点対象のセグメントの中での連携として、インフルエンサーを通じた発信、自己組織を通じた横連携などが促進できれば、より有効な取組になると思う。（中西委員）

○重点対象として世代と個人／企業が混在しているが、一度、メッシュでセグメントを整理して、強い部分・弱い部分を把握する作業をしてはどうか。（中西委員）

○本分野では、最新の情報をいかにアップデートしていくかが課題。（後藤会長）

（２）コーポレートガバナンスにおけるサイバーセキュリティの取扱いについて

事務局から資料２の説明を受けて、意見交換を行った。委員からの意見の概要は以下のとおり。

○経営者のサイバーセキュリティに対する Awareness 自体は、この１・２年で変わってきていると思う。SC3 等の活動を通じた具体的な事例共有や、自社のマテリアリティ（重要事項）への位置づけ、企業の非財務価値に対する評価指標への位置づけもみられる。強制力をもったアプローチだけではなく、このような他社事例の共有を促進して経営者に呼びかけることも効果的ではないか。（志済委員）

○企業・金融機関内の経営層への説明が、事業へのインパクトに関する説明まで及んでおらず、経営と現場の間で現状認識に関するコミュニケーションが円滑に進んでいない。現場が説明方法を工夫する必要があるが、業界ごとに事業へのインパクトに特性があることや、BCP 対応が自然災害の場合とは異なる点に注意が必要。（鎌田委員）

○所謂「名ばかり CISO」が多いが、フルタイムで会社としての組織的課題を解決するリーダーシップが必要。経営企画部門などがイニシアチブをとってサイバーセキュリティ対策を進めることを促進すべきではないか。（鎌田委員）

○地方拠点と本社とのガバナンスレベルの差が大きいという議論があるが、グローバルビジネスではその差がより顕著である。買収した他国企業のセキュリティ対策が不十分で、インシデント発生につながるケースもあり、海外拠点とのガバナンスレベルを揃える動きが出てきている。（蔵本委員）

○サプライチェーンセキュリティについては、米国大統領令のような、強制力のある仕組みが必要ではないか。近年自動車業界のセキュリティが進んだ背景として、法規制化された点が大きい。（蔵本委員）

○米金融機関では、女性役員が一定数いないと IPO 支援しないルールを設けている企業がある。同様に、有価証券報告書上でサイバーセキュリティに関する記載がなければ金融機関から IPO 等の支援を受けられなくなるといった、インセンティブ設計を考えてもよいのではないか。（蔵本委員）

○前所属の飲料メーカーでも、自社が踏み台になることで、サプライチェーンに影響を及ぼすリスクやブランド毀損リスクは懸念事項であった。リスクは会社の事業等で変わるが、そのリスクの定量化が難しい点が課題と感じる。（島委員）

○サイバー攻撃のリスクを懸念し、対策・体制に関する情報開示を避けたがる企業があることが課題。対策状況に関する外部評価機関を政府にてオーソライズし、診断結果を開示させて自社の目標設定を促すような取組も考えられるのではないか。（島委員）

○「セキュリティはコストではなく投資」というメッセージについて、サイバーセキュリティはコストではあるが、企業経営の中で吸収して、事業を推進する必要のあるものというメッセージを出した方がよいのではないか。（下村委員）

○セキュリティ対策を可視化し、リスクコミュニケーションに活用されることが重要。米国では対策状況の可視化ビジネスが定着しつつあるが、日本でも同様にビジネス化を進めないと取組が広がらない。（下村委員）

○中小企業の経営層に対しては、サイバーセキュリティはBCPの一環として訴求した方がよいと思う。「コーポレートガバナンス」という言葉は、中小企業には関係ないと言われてしまう懸念がある。（下村委員）

○企業としてまずやるべきことは、経営層を含めた階層ごとの知識付与だと思う。研修プログラムが整備されてきているので、これらの活用を促進すべき。（三浦委員）

○その上で、サイバーセキュリティに取り組むことが市場から評価され企業価値向上につながるようなインセンティブ設計も重要。DX認定は、一歩前進と思う。（三浦委員）

○現状で開示されているスキルマトリクスには、ITやデジタルすら十分に記載されていない状況だが、サイバーセキュリティは独立した経営リスクとして認識されるべき事項と認識。気候変動対応に関する取組を参考に、非財務情報の一部としてサイバーセキュリティに関する開示を求める、内部統制の一部として位置づけを明確化することなどが考えられる。（三浦委員）

○情報共有については、産業別のISACが存在するが、縦割りの枠組みであり、業界横断的な情報共有の枠組み充実も検討していただきたい。（三浦委員）

○グループ会社を傘下に多く抱えている企業では、サイバーセキュリティが重要な事業リスクであるグループ会社が存在しても、グループ全体としての有価証券報告書の記載は簡潔になっており、リスクの把握が難しい。投資家に必要な情報開示項目が必ずしも明確ではなく、整理する必要がある。（藤本委員）

○気候変動対応に関する開示の枠組みについては、企業と投資家との間の長い対話により実現した。サイバーセキュリティに関しても、企業と投資家との対話を促進する取組が重要。（藤本委員）

○近年コーポレートガバナンスの観点で企業に対応が求められている気候変動対応やダイバーシティといったトピックに比べて、サイバーセキュリティは見えやすい・わかりやすい到達目標の設定が難しい。リスク分析の中でサイバーセキュリティの優先度を高める観点から、各種ツールやガイドラインをアピールし、投資家との対話に活用してもらうことが第一歩ではないか。（中西委員）

○産業界だけでなく官（地方自治体）や学（教育機関）でも、それぞれの経営層へのアプローチが必要ではないか。（野口委員）

○経営者の意識をもう一段高める必要がある。米国では、サイバーセキュリティが適切に実施されていないと、投資家から企業の継続的な売上・利益を毀損するとみなされるが、日本の機関投資家からは、企業に対して明確な要求が出されていない点は課題だと思う。また、全米取締役協会と意見交換した際に、米国では M&A 時にサイバーセキュリティ・デューデリジェンスが行われていると知り、驚いた。（八剱指導専門官）

○身近な事例でも、事業継続に影響を与え得るようなランサムウェア被害が増えてきており、企業にとって「今そこにある危機」になっている。日本では、東証が示す「コーポレートガバナンス・コード」を意識している上場企業が多いが、本文書の中でサイバーセキュリティに関する項目を位置づけ、経営層の意識向上に向けたインセンティブをつけることが必要ではないか。（八剱指導専門官）

○米国でのインシデントに関する調査を通じて、米国では、セキュリティ格付け専門会社が、非常に高度なセキュリティ技術者を抱えて分析していることがわかった。このような格付けがビジネスとなっており、デューデリジェンスのために高度な人材が求められている点が印象的であった。（後藤会長）

○サイバーセキュリティを BCP の観点で捉えることが重要だが、個別の企業への直接的影響だけではなく、社会、産業への波及的影響についても、産業連関表を用いて分析する試みを行っている。このような経済学の専門家とのジョイント・プロジェクトにより、投資家・経営層の意識を向上できる可能性がある。（後藤会長）

（３）人材育成等に関する取組状況について

事務局から資料 3 の説明を行った。（意見交換の時間は設けなかった。）

以上