産業サイバーセキュリティ研究会 ワーキンググループ2(経営・人材・国際)(第8回) 議事要旨

1. 日時・場所

日時:令和4年3月23日(水) 10時00分～12時00分

場所:Web開催

2. 出席者

委員 :梶浦委員(座長)、熱海委員、岩下委員、小原委員、佐藤委員、武智委員、塚本委員、土佐委員、
名和委員、藤原委員、丸山委員、森川委員、湯浅委員(欠席)、松原様(横浜委員代理)

オブザーバ:内閣官房 内閣サイバーセキュリティセンター、金融庁、総務省、厚生労働省、文部科学省、
デジタル庁、独立行政法人情報処理推進機構

経済産業省:大臣官房 江口サイバーセキュリティ・情報化審議官、商務情報政策局 奥田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

事務局から、現下の状況を踏まえて、本日はオンライン(Web)開催との発言があった。

開会にあたり江口サイバーセキュリティ・情報化審議官から挨拶があった。

梶浦座長が、議事進行を行った。事務局から、湯浅委員は欠席、また、横浜委員の代理として松原様が出席の発言があった。次に、本日の議題に入り、事務局より資料3の説明に続いて、以下のとおり自由討議を行った。

(1) 経営について

- ・ 経営層側の理解が不足しているのではないかと指摘もあるが、業務だけではなく、システム自体も既存システムを含め複雑化しているところもあり、経営層と担当者両方のレベル、スキルを上げていかないといけない。企業が脆弱性に対してどのように対応しているかスコアをつけて一定の評価をするということがスタンダードになってきている。攻撃を受けたときにどのように対処するかというよりも、被害を受ける前に何か対策をしておかないといけない。
- ・ 儲けるセキュリティ戦略を出して良い時期ではないか。デジタルガバナンス・コードの4項目(ビジョン・ビジネスモデル、戦略、成果と重要な成果指標、ガバナンスシステム)の中で、セキュリティは「ガバナンスシステム」に入っているが、2番目の「戦略」に位置づけて、なぜサイバーセキュリティをやるのか、誰のためにやるのか、戦略としてサイバーセキュリティをやる意味は何かということを会社として整理する、そこが出発点ではないか。そのためには、セキュリティリスクを定量化し、例えば被害が一定以上になったときは、誰の責任になるか等を突き詰めて、戦略として考える必要がある。また、グローバルなサプライチェーンの議論もしなければならない。このためには、本事務局資料の英語化も含めた英語での情報発信・コミュニケーション、サプライヤーとの契約交渉に係る考え方の整理、サプライヤーを選ぶ基準としてのベンチマークの導入が必要。
- ・ サイバーセキュリティは企業のビジネスリスクの一部であり、例えば地震なども含めた一般のリスクと同等に扱うセンスが必要。これまで、サイバーセキュリティは情報部門やセキュリティ部門に対して「一義的責任」があるという考え方が主流だったが、それが経営の課題であるというメッセージが出てきて、ビジネス上のリスクとして、ビジネス部門が「第一義的

責任」を負うべき状況になってきている。この意識を浸透させていくことが重要であり、経営ガイドライン等にも盛り込むべき。

- ・ 経営ガイドラインの改訂について、9番目の指示である「サプライチェーン」が何を指しているのか。例えばバリューチェーン・物流、ソフトウェア構成部品、あるいはネットワークの接続など様々な捉え方がある中で、漠としないよう、それらを分けて説明すると、経営者が何をしたら良いかが分かりやすくなるのではないか。また、8番目の指示である復旧について、現在のガイドラインには、事案を防ぐために事前に何をすべきかが書いてあるが、昨今の状況鑑みると、事案が起きた後に直ちに復旧するため事前に何をしておくべきかについて焦点を当てて書くべき。経営者が一番困るのは、ビジネスが止まってしまうことなので、どのように備えておくべきかについてももう少し強調した方がよい。記載順も8番目ではなくて、さらに前に持ってくるのも一案。
- ・ 経営ガイドラインの改訂において考慮すべき状況変化については、昨今のウクライナ情勢について少し触れるべき。また、経営者に発信していくべき情報については、経営者の「善管注意義務」という法適用性に訴えかける形を取っていくのはどうか。現在サイバーセキュリティを巡る様々な係争があるが、その中で、サイバーセキュリティ対策とは、企業にとって競争力の源になり得る技術やノウハウ、顧客情報や取引に関する情報、連絡先も含めて、安全に確保した上で有効に活用するためのものという定義が表現を変えながら記載されており、そのような定義・解釈も反映していくべき。
- ・ サイバーセキュリティ経営ガイドラインの改訂にあたっては、ぜひDX with Securityのコンセプトや重要性を全面に打ち出していきたい。何らかの基準を求めている企業も多いことから、JCICでも「社内のセキュリティリソースは0.5%以上を確保せよ」というタイトルのレポートを先週公表した。このような取り組みも参考にいただければ。
- ・ サイバー空間とフィジカル空間が融合する中で、リスクについてもサイバーフィジカルの融合を考えることが重要。また、サイバー空間のリスクの状況は、おそらく経営者が考えているリスクの認識よりも先んじており、経営者に対し、より強くサイバーリスクについて意識するように働きかけることが重要。その意味で、投資家やその他のステークホルダーに対しリスク開示を積極的にするよう働きかけることは重要であり、特に投資家にとって重要なことについては有価報告書やESG報告書にリンクさせるのもひとつの手段である。米国でもForm 10-KやForm 8-Kに記載すべきというような話が出てきており、日本企業も影響すると思うが、そういった動きも認識しながら国際連携をしていく必要がある。
- ・ 経営ガイドラインについて、タイミング次第だが、経済安全保障推進法案の内容も反映させるか、あるいはクロスリファレンスする形で企業が混乱しないように文言を作っていた方がよい。
- ・ 政府からの注意喚起について、受け取る側がどのようなアクションを取るべきかを明確化するためには、サイバーセキュリティについて必ずしも知見のない経営層あるいは中小企業向けと、現場で日々脅威と戦わなければいけない人向けと、それぞれに対する情報発信の仕方を分けた方がよい。例えば、米国CISAのShields Up等は、経営層向けには具体的な国がどういったサイバー攻撃をしているのかというストーリーが分かるもの、現場向けにはIoC (Indicators of Compromise)や脆弱性情報などの細かい技術情報を分けて発信している。また、Emotetを含め脅威が増している中で、当然、企業側も防御努力を強化しなければいけないが、全てのサイバー攻撃からの侵入を防御しきることは企業にとっては不可能な時代に突入している。高度な技術を持った国家によるサイバー攻撃が増えている中で、日本政府は企業にどのような支援をするのかも合わせて記載し、官民一丸となって戦うという姿勢を示していただいた方が民間企業もやる気が出るのではないか。

(2) 中小企業対策について

- ・ この5年間に、サイバーを利用することの必要性や世の中のデジタル化の動きは一段と進んだにもかかわらず、セキュリティ対策の必要性を感じない企業が2割という状況が、いまだに続いている。実際には、このアンケートに回答しなかった人も含め、世の中には「サイバーセキュリティは、自分とは関係のない話で、特定の特殊な情報を扱っている企業のことだ」と思っている人が多いと思う。実際、その中の実に7割にあたるどころが重要な情報を保有していないと回答しているが、今時重要な情報を保管していない企業など存在しない。

- ・他方、国際的に比較をすると、日本の企業、特に中小企業のデジタル対応への遅れが日本の競争力を大きく削いでいるということは、統計的にも明らか。仮に各企業が、サイバーセキュリティ対策を講じたくないからDXに対応しないという形になっているとすると、サイバーセキュリティ対策を強調すればするほど、むしろDXを企業から遠ざけてしまい、結果として、生産性が落ちてしまうという問題も招来しかねない。その点を勘案しながら、車の両輪としてDXの進行とサイバーセキュリティの向上というのは両方必要であり、両建ての作戦、両面作戦をぜひ進めていただきたい。
- ・大企業と中小企業の連携について議論があったが、具体的に、発注元の企業やサプライチェーンの頂点の企業がサプライチェーン全体のセキュリティ対策について、どのような取組をしているかの事例の横展開ができないか。サイバーセキュリティお助け隊についても、発注元の企業からの紹介で中小企業が利用を開始したという例を聞いており、業界団体を通じて橋渡しをしていただくことは、ひとつの手掛かりになる。
- ・経済産業省が働きかけをしている「パートナーシップ構築宣言」の枠組みの中で、サイバーセキュリティ対策を進められないか。ひな形には、IT化の支援や脱炭素化に向けた取組などがあるが、まずはここにサイバーセキュリティ対策をぜひ入れていただきたい。
- ・SC3やサイバーセキュリティお助け隊サービス事業を通じて、中小企業でのセキュリティ対応は、意識やコストの問題があり非常に難しいと常々感じている。日本の産業のセキュリティレベルを上げるためには、99.7%を占める中小企業のセキュリティレベルを上げていかないといけないことは明らか。現状、中小企業のセキュリティに対する具体的な施策としては、お助けサービス以外は抽象論が多い印象であり、先行しているお助け隊サービスをいかに上手く活用するかが重要。
- ・既に様々な支援活動や啓発活動は行っているのだから、後はどうやって当事者意識を持っていただくか。例えば、きちんと対策を講じていればある種の免責がある、もしくは調達上の特典・加点がある等のインセンティブや、きちんと対策を講じていなければ調達に入れないといったものを組み合わせて具体的にを見せていくと少し変わるのではないか。米国のFCPA（海外腐敗行為防止法）でも、対策をしていると公表されなかったり、もしくは罰金が減額されたりすることがある。また、“i-construction”で、国交省の直轄工事にはICT導入が必要になったと同時に、ICTのマシンの購入に補助を出すことで、アメとムチで、中小建設事業者までICTの活用を浸透させていったという例がある。加えて、プライバシーマークがいくつかの自治体で調達の際に必要なことでマークが広まったこともある。何らかの形でやらないといけない気持ちにさせるものがあると良い。また、DX銘柄、なでしこ銘柄、健康経営銘柄等、経産省も様々な表彰制度を有しているが、セキュリティ対策をグループ全体で上手にやっているところを表彰する制度があれば、ベストプラクティスが集まる上に、企業自身にとってもプラスのインセンティブになる。
- ・大企業から見えるサプライチェーンは限られており、ほとんどのサプライチェーンは中小企業間で形成されている。自分の対策も必要ないと思っている企業が、取引先に対して何か要請することは想定されないため、それぞれの意識を変えてもらわないと、サプライチェーンで対策が広がることはないだろう。しかし現実的には、情報を取られても会社は潰れないと思っている人が多いのではないかとと思われることから、会社が潰れるという点にもっとスポット当てて、リスクの方から話をしていくことが一案。ここ2、3年でランサムウェアの事例が出てきており、それを取り上げていくのがよいのでは。
- ・現実的な対応としてはお助け隊のようなものが必要だが、そのハードルを下げて、入会金無料などのようなものから始めないと普及しない。ただし、その際のコストを誰が負担するのか、公共事業にするのか、大手の業界団体がある程度は業界内で負担するのか等、コストの工夫も検討が必要。また、ハードルを下げることにより、少なくとも何か対策を取ろうと思っていた人は対策を始めると思うが、もともと全く対策を取らざるを得ない人に対策を取らせるためには、対策を取ると得する等のインセンティブがないと難しい。こうした取組を実施する際に、必要となるのが評価制度。第三者が評価し、中小企業の皆さんのレベルを明らかにする仕組みがないと、前に進まない。また、対象となる中小企業についても、受注はFAXで受けています、帳簿は全部紙でつけています、制御装置はスタドアローンですという会社はサイバー攻撃被害が限られるのではと思うので、中小企業99.7%とはいっても重点的に対策すべき企業は絞られる。

- ・大企業からの支援について、例えば、本社からグループ会社に対して支援を行うときに、コストは本社の費用で落として良いのかという点が曖昧。これは子会社を守っているのではなく、本体自身を守っているからコストになるという論法もあるが、若干曖昧であり、対策費用は税制上費用に計上されるのか、もしくは子会社側に応分の負担をさせなければいけないのかという点が明確になると対策を実施しやすい。親会社のコストにはできないことが明確になれば、例えば子会社に増資・融資等を行う等の別の方法も取り得る。
- ・中小企業のセキュリティアクション、あるいはお助け隊サービスなどについて認知度がまだ低いという話があったが、認知の向上プロセスは2段階あり、まず第1段階で言葉自体に耳をなじませる、そして第2段階で、聞き覚えのあるその言葉が、実際何なのかを知らせるというのが定石。その際のツールとしては、地方や企業規模が小さいところでは、ウェブ広告よりも、テレビやラジオが圧倒的に有力な媒体。ラジオ等と合わせて、金融機関等の支援策を出してパッケージ化するのが効果的。
- ・よく、お金をかけられないから中小企業は簡単なセキュリティ対策で良いといった話が出るが、必要なセキュリティ対策をするのに中小企業かどうかは関係ないという点は申し上げたい。中小企業については、社会的に2つの問題を整理すべき。一つは、産業サプライチェーン上の中小企業。これは、OEMのビジネスレジリエンスの問題であり、OEMが責任を持ってレジリエンスを確保することを義務づけ、意識付けすれば解決するのではないか。ただし、自主的では上手くいかない、時間がかかるということであれば、政府が補助金や規制を使い、アメとムチで補正をすることが有効。もう一つがベンチャー企業。これは、秘密保持の問題。ベンチャー企業の技術は、場合によっては軍事技術に使われる可能性もあり、安全保障の観点からも、貴重な技術情報を敵対的な勢力に取られて競争力上不利になることを避ける観点からも、秘密保持による便益を得るのが日本国民一般と考えると、国が積極的にそのようなセキュリティ対策をするための方策として、補助金を付けるなどは考えられる。
- ・セキュリティ対策ということで企業を大きくふたつに分けると、対策に関心がある企業と、そうではない企業に分かれる。対策に関心がある企業は、これまでは情報化が優先されて、セキュリティ対策がなかなか進められなかったという事情があり、例えば補助金制度や金融機関等によるインセンティブ付けをすることが有効と考える。現状では、セキュリティ対策だけを対象とした補助金制度はほぼないと認識しているが、そのような制度により、たとえばお助け隊などは有効に機能していくのではないか。関心がない企業については、どのようにして経営層を変えていくかが重要だが、プライバシーマークが自治体等の調達要件になり普及した例のように、セキュリティ対策が企業の評価制度の一部になるという発信をしていくことで、対策をせざるを得ない状況になるのではないか。また、中小企業が加害者になる可能性も大いに秘めており、対策の甘い企業はサプライチェーンからも排除されうるということを理解していただくことが重要。
- ・セキュリティ対策を推進していく母体は、もちろん商工会議所等地方という観点もあるが、業種業態によっていろいろ取り組むべき課題は変わってくることから、同じ業種や業態の中で連携して対策について取り組んでいくことが重要。

(3) 人材について

- ・人材に関しては、戦略的な視点が必要。まずは、インテリジェンスサイクルを回せるかどうかという点。事故があった際、対処だけでなく、なぜ起きるのか、どこに原因があるのか等について、きちんと情報を蓄積・分析し、それを改善につなげていくという当たり前のことがきちんとできるか。また、インシデントレスポンス演習においては、異なる文化や国とのやりとりの中で、きちんと自分の言う通りにベンダーやサプライヤーが動いてくれるか等に踏み込んでいく必要がある。そのためにもセキュリティ言語は統一すべき。3月1日の経済産業省からの注意喚起についても、技術寄りの印象。経営者に受け取ってもらうためには、戦略的にプロセスや人材について何をしなければいけないのかというメッセージが必要ではないか。
- ・デジタル機能の構築やツール開発の実施や説明責任は、IT部門ではなくビジネス部門に持たせるというケースが最近増えている。いわゆるノーコードなども含めて、ビジネス部門がデジタルデリバリーをするということが主流になりつつある中で、事業部サイドがITやセキュリティに関する人材を抱える必要がある。特に米国等では、ほとんどの企業におい

てIT部門よりもビジネスサイドにIT人材が多い。こうした考え方が、SC3やサイバーセキュリティ戦略等を出ているプラス・セキュリティの重要性に通じる状況だと考える。ただし、残念ながらプラス・セキュリティをどのように育てていけば良いかという具体策がまだまだこれからであり、ここをどのように進めるかを考えていくことが必要である。

- ・いろいろと議論する中で、いつもぶつかる問題は人事制度である。昨今、メンバーシップ型からジョブ型という話になってきているが、米国等では、ジョブ型はいわばポジションが決まると給料が決まるものだが、日本のジョブ型では、同じポジションでも給与が違うところがある。ジョブディスクリプションと給与体系がタイトには繋がっていない人事制度において、セキュリティ人材やプラス・セキュリティの能力を持った人たちをどのように評価するかという点は難しい。他方、これはセキュリティの問題だけではなく、DX人材という、要はデジタルデリバリーができる人材をどのように評価していくかという問題でもあり、要はビジネスへの貢献度をどのように測るかという問題を解決しなければ、プラス・セキュリティを反映できる人事制度にはなっていないと考えている。
- ・プラス・セキュリティについて、どの層に対して何をやろうとしているのかを、もう少し明確にすべき。例えば、セキュリティ統括層や戦略マネジメント層等の育成に必要な教育は明らかであり、また、全社員が最低限理解しておくべき点はe-learning等で啓発している。他方で、プラス・セキュリティについては、例えばコーポレートコミュニケーション部にとっては、インシデントが起きたときに、どこに対してどのような発信をするか、どのようなタイミングでリリースするかが分かることであり、法務部にとっては、契約にセキュリティについてどのように盛り込んだら良いのかが分かることであり、営業部にとっては、顧客との共同作業でユーザーIDとパスワードを共有するとなった際に社内の然るべき部署に相談しないと危ないと気づくセンスを持っていることであると思う。プラス・セキュリティがいかなるものかということ、もう少し分析的に書いてもらえると、関連の教育や枠組みが広がっていくのではないかと。
- ・プラス・セキュリティについて、インシデント現場の支援に行くと、共通言語はサイバー脅威やサイバー攻撃ではなく、法的要請となっている。支援する側も支援を受ける側も、法的な理解が必要であるが、弁護士もサイバーインシデントについては不慣れなところがあり、カオスな状態になることがある。昨年9月28日に閣議決定された「サイバーセキュリティ戦略」において、「「プラス・セキュリティ知識」を補充できる環境整備」に、「対策推進に向けた専門人材との協同等に資するよう、法令への理解を深めるツール等の活用促進を図る」との記載がある。まさにこれを進めていくことが、現場の対処の迅速化につながるのではないかと。
- ・プラス・セキュリティ人材の普及について、IT部門やセキュリティ部門主導だと、なかなか動かないという問題がある。企業でこれを推進していくにあたってのキーポイントは、やはり人事、総務、営業など、そういった非IT系部門を初期の段階から巻き込んで、共に考えながら、彼らに納得してもらいながら計画を練ることが重要ではないかと。ここは経営層の配慮が必要な点だと思う。また、現時点でも事業部門にプラス・セキュリティ人材のような方々は既に存在しているものの、大抵ボランティアの扱いをされていることが多いのではないかと。人事評価でプラスがつくようにしないと、プラス・セキュリティ人材の広がりが望めないことから、経営者の方々にも、そういったところを後押ししていただくことが必要なのではないかと。
- ・フィジカル空間とサイバー空間のリスク認識は同じであることを考えると、人材育成もサイバー空間だけを知っている人というよりも、全体を通じて理解する人が必要であると考え。結局、すべての人がサイバー空間に関わってくるわけで、そうすると、年齢、業界、所属組織、役職に関係なく、自分の仕事や自分の生活に必要なセキュリティの知識を得ないといけないということになる。子どもであっても大人であっても、例えばiPadを使うとなったときに、必要なセキュリティ知識は身につけるべきだと思う。
- ・プラス・セキュリティ人材という名称では、サイバーのことをプラスして知っておけば良いという印象になってしまうところがある。名称としては良いが、サイバー空間を使うのであれば、当然そのリスクについては、誰であっても知っておかないといけないというような認識を広めていく必要があると思う。この役職の人に少しセキュリティのことを知ってもらいましょうというのではなく、知ってもらうのが当たり前で、どういうことを、どのように理解してもらいましょうかということが議論の中心になっていくべき。そして、必要な人にサイバーリスクと対策についての情報がアクセスできるような環境を整備

することが重要である。

(4) 地域について

- 各地で様々な取り組みが既になされているが、当然ながら地域により活動状況や広がりには濃淡があると思う。デジタル田園都市国家構想をきっかけに、大学や自治体、地元企業等と話す機会が増え、改めて連携が深まっている。地域の大学も含めて産学官でコンソーシアムを作っていくような公募のようなものがあると、改めて地域で何をすべきかという議論が各地ではじまると思う。その際に、例えば地域の大学で人も雇えるようにしていただくと、人材の流動化や地域の活性化にもつながる。また、当然ながら、大学自体のデジタルに対する意識向上にもつながるため、そういったことも検討していただければどうか。
- 各地域では、経産省、警察庁、総務省といったガバナンス主体があるが、もう少し警察、総務省と連携し、支援すべき中小企業の対象領域を拡大すべき。関係省庁で、共同でプロダクト、レポートを作り、提供すると、相乗効果があるのでは。米国や英国はすでにこのような省庁間連携を始めており、そろそろ省庁間で緊密な連携を行い、限られた予算・人材を有効活用していくべき。
- 地域の特徴は、物理的な近接性であり、日頃の地域コミュニティの中で、セキュリティに対する意識啓発などが重要になってくる。例えば、防犯分野では、地域でおかしなことがあったらアラートが上がるような仕組みがあるが、サイバーセキュリティについて、何かおかしなことがあった時に、日頃のコミュニケーションの中で相談できるような窓口のようなものがあれば良いのでは。すでに、産官学連携はネットワークとして存在しており、学のネットワークや地域のネットワークを活用することが、地域社会においては重要。

(5) 国際について

- サイバーセキュリティを国際で取り組む上では、インテリジェンス情報との付き合い方も重要な論点。各社の経験を共有する場の在り方も検討いただきたい。事業の中で入手した情報について、経営者にも共有するか、「公助」と「自助」のバランスの中でどのように付き合うか、企業はどのような公助を期待できるのか、あるいは官の側もプライベートセクターからのどのような情報を欲しいと思っているのか、その辺が明確になってくると良い。
- 「特にフォローすべき海外の動向、連携すべき海外の機関等」について、インフォメーション・セキュリティ・フォーラム (ISF) は非常に有益なので経産省として入られたらどうか。各国のセキュリティ関連の公的機関、最近ではデンマークのセンター・フォー・サイバーセキュリティも入会している。セキュリティについて取り組む人たちを横できちんと見た上で国際的な問題を考えていくべき。
- JPCERT/CCが最近、ブログ等において英語で、一般や情報システム部門向け価値ある知識を頻度よく提供している。ICSCoEの国際プレゼンス向上にあたっては、例えば産業領域のエンジニア向けの脅威レポートや洞察等を少し本格的に作っていただき発信していけると、他の国に喜ばれたり、または共同活動のきっかけとなったりするのではないかと。
- 国際的な連携は、セキュリティ対策をとるという観点では非常に重要になってくる。特に、どのような国と連携するかが重要になるが、米国は同盟国なので連携することは必要として、それ以外にも考え方や思想が近い、例えば民主主義的な価値観を共有する国と連携することは重要。特に、米国ではトランプ大統領のときに久しぶりにセキュリティ戦略を出したが、EU、ドイツ、オランダ、英国、オーストラリア、カナダ、それから、QUADのようなことを意識するのであればインドといった国も、セキュリティ戦略を考えている。特にインドは、レジエンスに力を入れている。各国の戦略と平仄を合わせて進めていくべき。
- 日本がサイバーセキュリティ対策をしっかり行い東京五輪を成功裏に終えたことや、お助け隊や各地域における商工会議所がすぐれた取り組みをしていることは、海外で必ずしも知られていない。サイバー攻撃の脅威が高まっている今こそ、日本の知見を世界に向けて英語で発信すべき。それにより日本のプレゼンスは高まり、世界のサイバーセキュリティ強化に貢献できる好機ともなるのではないかと。

お問合せ先

商務情報政策局 サイバーセキュリティ課

電話：03-3501-1253

以上