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10回）
議事要旨

1. 日時・場所

日時：令和6年3月25日（月） 10時00分～12時00分

場所：ハイブリッド開催

2. 出席者

WG2委員　：梶浦委員（座長）、熱海委員、小原委員、佐藤委員、武智委員、塚本委員、土佐委員、名和委員、原委員、藤原委員、丸山委員、湯淺委員、松原様（横浜委員代理）

オブザーバー　：内閣官房内閣サイバーセキュリティセンター、警察庁、金融庁、総務省、外務省、厚生労働省、農林水産省、防衛装備庁、デジタル庁、独立行政法人情報処理推進機構、国立高等専門学校機構

事務局　：経済産業省 上村サイバーセキュリティ・情報化審議官、武尾サイバーセキュリティ課長、山田サイバーセキュリティ戦略専門官

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、資料の確認を行った後、資料3の説明を行った。以下のように自由討議を行った。

＜1. サプライチェーン対策について（中小企業・地域、経営）＞

- サイバーセキュリティの確保に向けた各種の取組を我が国産業競争力の強化につなげることが今後の課題であり、高い評価につながるアイデアや仕掛けを考えるべき。そのためには具体的な数字のイメージや見せ方については議論が必要。例えば、セキュリティインシデントによる被害を踏まえた費用対効果などが重要。400 万社の中小企業に対策を実施していただくためには、何らか有効な説明が必要。日本におけるサプライチェーンの規模は世界有数であり、競争力の源泉である。サプライチェーン全体のセキュリティ対策強化は利益の源泉を守ることになる。そのようなメッセージが欲しい。

- 経営陣に対してお金の議論は必要である。例えば、過去の TSMC での 3 日間の操業停止によって、190 億円の損害が発生したと記憶している。そのような具体的な議論がなければ経営陣に刺さらない。
- 過去に発生したとある決済サービスにおける事例では、公表された被害額は 3,800 万円となっているが、問合せの体制を作るなどの二次的な費用を含めると 40 億円程度の被害が出たと伺っている。

- 施策については、十分に成果が出たものは継続し、課題があるものについては改善を図ることが重要ではないか。
- 施策の方向性には自助、共助、公助が整理されていると抜け漏れなく検討ができるのではないか。公助がほぼ見られないという意見も伺うが、経産省は経済の推進、促進を主眼とおいている点は理解しているため、公助と自助のバランスをとることを期待する。

・ IPA や JPCERT/CC をご存知ない事業者は一定程度いる。運輸、農業、ホテルを含む分野でそもそもセキュリティに馴染みのない方が多い印象で、380 万社あるアクティブな中小企業のうち大半がそのような状況ではないか。以前、ある報道機関の番組制作支援にかかわったが、「マルウェア」と書くとわからないので「ウイルス」に直された点からも認識の不足が感じられる。キャンペーン不足と思われるので、もう少し踏み込んで対応されるとよい。

・ 産業全体で全てのサプライチェーンを対象にすると、それぞれの最も弱い部分を底上げする施策の検討だけでも時間がかかる。守るべきサプライチェーンに優先順位をつけ、例えば、特定社会基盤事業者から始めるということなども考えるべきではないか。
・ 中小企業におけるセキュリティの底上げは、対面で実施しなければ広がらないと考えられる。どんな事例や被害額を見せても、そのインシデントが自分のところでも起こると感じてもらわなければ、対策する気にはならないのではないか。
・ 中小企業と言っても、本件では個人事業主ではなく法人を対象にしていますというように、企業の規模やサプライチェーンに占める位置づけなどをより詳細に検討して、スコープを明確にしていただけると結果を早く出せるのではないか。

・ 施策は大枠にとどまるのではなく、解像度をもっと上げる必要がある。その場合にはどのような業種、規模が重要かという議論がある。また、その際、業界団体が本気になっているかという点も考慮する必要がある。
・ 今年に入って経産省では、企業成長促進のための政策の一環で、中堅企業者を定義した。中小企業のうち中堅企業は 9,000 社ほどある。中小企業者がセキュリティ対策を実施する際に人材や金の不足が指摘されているが、中小企業よりは金は不足していない中堅企業を対象に施策に取り組んだ上で、順次トリクルダウンしていくという考え方もある。
  中堅企業を対象にするにあたり、プラスセキュリティとして、業務の一部としてセキュリティ対応を行なっている実務者を束ねる役割を持つ部署を総務部門等に必ず設置することを推奨することも一案。

・ 規模等に応じたセキュリティ対策の提示は非常に重要な観点である。昨年 7 月の東京商工会議所の調査では、サイバーセキュリティについて、「十分に対策している」、「ある程度対策している」という企業が、80%以上となっていた。しかし内容を伺ったところ、ウイルス対策の導入、ソフトウェアのアップデートが突出して多く、社内教育、セキュリティ診断又は訓練の実施など他の項目は 3 割以下となっている。基礎的な対策を実施しているが、それで十分かどうかは議論が必要である。小規模企業では十分かもしれないが、中堅企業等では不十分の可能性がある。

・ 既存の制度が着実に成果を上げている点を評価する。大企業の立場からすると、取引先や仕入れ先でサイバーセキュリティ対策がどの程度なされているかを正確に評価することがまだまだ難しい。様々な企業から異なるチェックリストが届いて対応が煩雑であったり、現地監査も一部の例外を除いて効率的とは言えなかったりと課題も指摘されているところ、業種横断のチェックリストやガイドラインを産業界全体で普及することが重要と考える。
・ 取引先企業に実施状況等を求める点について、経済産業省及び公正取引委員会から「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」として考え方が定義されたが、取引先にどこまで要請できるのか不明確のためケースバイケースの対応となっている。何かしらガイドライン等があれば、大企業からセキュリティ対策の促進支援や要請等が可能になると考えられる。

・ 人権デューデリジェンスの取組を行わなければビジネスに支障をきたす場合があり、大企業が取引の際にチェックする必要が生じている。セキュリティも同様に大企業側から取引先に要望できるようになるとよい。政府調達の中にセキ

ュリティを入れ込むこともよいが、必須の取組ではなく、大企業が取引先と一緒に取り組めるような土壌があるとよい。その意味では、セキュリティ対策の成熟度を可視化する取組は評価できる。

- 賠償責任保険の補償にサイバーリスクが含まれている場合、サイバーセキュリティ保険に加入する際に保険会社からチェックリストが提供されればそれが第三者チェックの役割を果たす可能性がある。

- ITに関する依頼事項が多いため、IT疲労を起こしているという経営層の意見がある。例えば、ツールやサービスを活用した事例の共有等、手っ取り早く具体的な方法を経営層に教えることが重要なのではないか。
- IT技術者とサイバーセキュリティ技術者は二分化していて、ユーザー企業にとって確保が難しい状況が続いている。インシデントが発生した際のレジリエンス確保のために、セキュリティ担当者の任命等を経営層へ依頼しており、その際は、総務や経理部署と兼任となってもよいとアドバイスしている。
- サイバーセキュリティ保険への加入を検討する際にはセキュリティ対策が可視化される。その工程が、企業がセキュアな状態になるための手段のひとつになり得る。

- 英米の動向をみると、サイバー対策が国家戦略と結びついている。すべての中小企業を対象とすることは難しいという点には同意できるが、基幹産業・重要産業は義務的な対応を求めるなど、施策の色分けをする必要がある。公助については施策の中小企業検討が難しい点があると思うが、そこがなければ具体的な議論が難しいため、メリハリを意識して検討いただければと思う。

- 広報的な観点としては、ロジカルとエモーショナルの両方が大事。ロジカルも必要であるが、エモーショナルの部分を推進していくことも重要。インフルエンサー活用等、広報的な面からも施策を検討されたい。

- 中小企業におけるセキュリティの確保は、法令で規定するなど強制力のあるものにしなければ対策の実施まで至らないと思われる。その意味では、日本における事業者の自主的な取組の促進は、中小企業にはフィットしない可能性がある。

- 「パートナーシップ構築宣言」の登録企業は、現在 43,000 社程度おり、付加価値向上のためサイバーセキュリティに取り組む企業も一定存在するので、その割合を上げるだけでも効果的ではないか。

- 下請けと元請けの関係を良くするための環境や人権の話を含め、どのようにして元請け側が下請け側とバリューチェーンやサプライチェーンを構築していくかという議論の中にサイバーが入り始めているところであり、KPI的な指標を活用するのであれば、どういう書き方が良いのか、どこまでお願いできるのかなどについて既存の施策も考慮しつつ議論することが必要。

＜2. 人材育成・国際について＞

- 人材不足に関するアンケート結果はよく見るが、毎年どれほど人材が雇用されているかを示す統計は見かけない。実際にどれだけ人材が足りないのか調べるのであれば、雇用状況に関するデータも集めるべきではないか。また、日本における今後の人材育成を考える上で、今までに産業サイバーセキュリティセンター(ICSCoE)から輩出された数百人ものトップ人材のキャリアが参考になるはずだ。スキルアップしたことで、彼らがどのようなキャリアパスを歩んできたのか、今後のキャリアをどう考えているのかをフォローアップすることで、人材育成に関する施策に活かせるであろう。
- 残念ながら、日本におけるサイバーセキュリティの取り組みについて、海外であまり理解が進んでいない。日本の対

策や能力が遅れていると断定的に言われることすらある。しかし、ランサムウェア攻撃被害に関する統計値を見れば、日本の方がはるかに被害を抑えられている。そうした統計や事実に基づき、日本がすぐに反論できない、あるいは国際発信できていないのも国益上問題である。

- 専門人材の育成にあたり、望ましい時期や時間帯、期間などについて結論として単一の答えはない。受講者を増やすにはバリエーションを増やす必要があるが、コストもかかる。
- 登録セキスペの維持費低減のためのコスト削減について、IPA の講習や教材のデザインやレビューを非常に多忙な方々がボランティアに近い形で対応しているので、コスト削減は困難である。自前の講座ではなく外部の研修機会も多くあるので、これを活用してポイント制にして講習受講実績とする等の案も考えられる。

- ユーザー企業が必要としているのは能力ある人材であって有資格者ではない。今のままの制度ではベンダーに登録セキスペが集中している現状からはなかなか変わらないのではないか。資格がなければ自社のビジネス・業務ができないような場合に企業は従業員に資格を取得させる。例えば、登録セキスペでなければ法定の監査業務ができないとする縛りを設けることなどの案が考えられる。

- 登録セキスペに業務独占を与えることは難しいため、例えば、調達条件への組み込み等の工夫をして資格取得の需要を喚起するなどが考えられる。
- 英国では 4 つのレベルのセキュリティ資格を設けているが、政府が独自にそれらのレベルを定義する代わりに、(民間等で使われている)既存の資格等をマップすることで、レベルを規定している。日本の場合は、既に登録セキスペという既存の資格もあるので、それを考慮する必要もあるが、バランスよく考えることが重要ではないか。

- ユーザー企業においてセキュリティ人材の不足は長年の課題である。経営者の意識が高まってきており、予算はつくようになっているが、人材が足りないと聞いている。中途採用はあるが、業界自体に人が足りていないところもある。専門人材はセキュリティ専門企業に就職するため、ユーザー企業での確保が難しくなっている。ユーザー企業としては、既存人材の育成に注力する傾向がある。IPA 中核人材プログラムについても、1 年間の派遣は負荷が大きいため、2 か月程度のプログラムがあるとよい。

- 10 年ほど前にデータサイエンスの取組みが広がり、政府からのサポートを受けて、学部の新設や必修科目の指定が行われた。セキュリティについても学部の必修科目とすれば、少子化により学生数が減ったとしても十数年の間は年間約 40 万人強程度は学ぶことができる。文科省と連携して取り組まれるとよい。

- 資料 3 の P.20 にあるように、保有しているナレッジに係る共通語彙の枠組みを米国(例: NICE Cybersecurity Workforce Framework(SP800-181)、CAE-CD)の取組を参照しつつ SC3 で整理している。デジタルバッジという形で個人の能力がわかるような取組を考えていただけるとよい。大事なのは、産官学にわたって関係する人・組織が共通した表現を用いて、人材、技術、知識や能力を表現することであり、それによって人材に関わるエコシステムがスムーズに回る環境を整えることである。

- 専門家向けの研修と、人事や経理等の一般向けの研修とでは、共通言語が離れてしまっている。データに関連するセキュリティ分野を各職種共通の研修内容として加えていくべき。
- 個人の専門スキルを全社員に認識いただくための場の設置を推進していくことも一案。

・ 中小企業の半数においてデジタル専任の担当者はいないので、ITベンダーやITコンサルへの相談が多い。一方で税理士や金融機関に対して相談を行うことも多いので、彼らからセキュリティの重要性を伝えてもらえることも効果的と思われる。

・ 大企業ではプラスセキュリティ人材の確保は進んでいるが、中小企業ではこれからという認識である。セキュリティ部門以外も含めて社会全体でプラスセキュリティ人材の確保を進めることが重要である。
・ 日本サイバーセキュリティ・イノベーション委員会(JCIC)では教育コンテンツの作成を進めており、非セキュリティ部門とセキュリティ部門が折り合える部分を示すべく検討を進めている。来年度にリリースできる見込み。

・ サプライチェーンの末端を支援する中で、その対象者に外国人が含まれ、最近増えてきている。公的機関が示す要件への適応などの難しい対応も、外国人が行うことさえある。専門人材に外国人も含めていくことを検討していただきたい。

・ 本来は市場原理で解決すべきところを市場原理以外で解決しようとしているから難しい。市場原理は強いので、優しいやり方では解決しない。法律にするか、資金を捻出するか、需給を市場以外でバランスさせなければならない。
・ 政策評価をより実効的なものにする必要がある。例えば、英国であれば、法律や政策の策定時に市場調査を行い、NAO(National Audit Office)という会計検査院にあたる組織が検査する仕組みがある。そのような取組を可能とするべく、経産省としてデータをしっかり揃えるべきではないか。

・ セキュリティ対策の成熟度の可視化の取組を達成するメリットを、インセンティブのある企業にとって元気の出るような書き方で示すべき。「パートナーシップ構築宣言」における各種補助金のようなものだとか、インセンティブ WG といったものを設けるような取組があるとよい。

・ 英国でも「Cyber Essentials 制度」というセキュリティアクションと類似の制度を運用しており、取得件数を KPI に設定していた。件数だけではなく、取得による業績の向上や新たな受注に結実したといった波及効果を KPI とすべきと指摘した際に、英国側もその旨納得していたようであった。

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