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9回)
議事要旨

1. 日時・場所

日時:令和5年3月27日(月) 14時00分～16時00分

場所:ハイブリッド開催

2. 出席者

委員 :梶浦委員(座長)、熱海委員、岩下委員、小原委員、佐藤健志委員、佐藤亘委員、武智委員、塚本委員、土佐委員、名和委員、藤原委員、丸山委員、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、警察庁、金融庁、総務省、厚生労働省、農林水産省、国土交通省、独立行政法人情報処理推進機構

経済産業省:大臣官房 上村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、佐藤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、資料の確認と委員の紹介を行った。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。

その後、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。

- ・ サプライチェーンにおける親会社をどのように支援するべきかを考えている。受益者が誰で、経費をどのようにかけていくべきか、法律に触れないか、もしくは経費を使用した後に会計検査等で何か問題が起きないかといった利益供与の観点をセミナー等で触れている。自分たちが悩み、どのように進めてきたかという経験を含めて議論したい。
- ・ 人材育成に関しては、業務遂行にあたり専門的技術を扱える人材を育成し、実際にクラウドを運用しながら会社で利用するための知識を習得させ、そこにセキュリティやネットワークの知識を蓄積していくといった方法も考えられる。2023年度以降、専門人材を有する企業と連携について相談していこうと考えている。
- ・ 日常的に情報セキュリティリスクにさらされている時代にあると言え、インターネットを使わないビジネスなど無い。一方で資料3のP.7では、セキュリティ人材の不足として日本だけ90%不足していると表れており、極めて憂慮すべき問題。
- ・ セキュリティ対策無しにインターネットを使っては駄目だと強く言うべきであり、セキュリティ対策を実施しなければ大きな罰則がかかる仕組みにしなければならない。セキュリティの損害は自身が損をするだけでなく、他者や地域の仕組みに非常に大きな損害が生じるということを考慮すべき。
- ・ P.8、情報関連のルールが無いという会社が中小企業で60%ある。法法令上、就業規則や定款が無いという会社は無いはず。未だにセキュリティは分からないと言う人たちを放置していることは、国の政策として大きな問題である。
- ・ 必要の無いセキュリティ対策を求めるのは優越的地位の乱用に当たるのかもしれないが、セキュリティ対策を実施して

いない会社と取引してはいけない。そろそろハードローが必要だという議論を政治の場で実施いただきたい。それらにあわせて人材を育成していくのは、アカデミアの仕事。

- ・ マクロな観点からの意見。本WG資料のなかでも、経済問題や規模の数値がわかる記載があるとよい。日本はどれだけの価値が損失しているかのイメージをつかみ、成功のイメージを描くことが重要である。そして、限られた予算を効率的に執行するには官民パートナーシップが必要で、経済安全保障の対象産業や経済的に勝機のある産業に優劣をつけることが必要。
- ・ 心の話、つまり倫理の観点からの意見。倫理とは守りの倫理と攻めの倫理があり、守りの倫理はやらないと罰則といったマイナスのイメージへ向かってしまうため、攻めの倫理である自律モデルへマインドセットを向けるべき。官民パートナーシップではどのようなシナリオにするか、を考えるべき。
- ・ シナリオの観点からの意見。業界に特化したインセンティブ設計と評価、あるいはリスクシナリオの策定支援がSC3に求められるのではないかな。
- ・ パートナーシップ構築宣言を行った1万社を超える企業のうち何社ぐらいがサイバーセキュリティを盛り込んでいるのか、あるいは具体的にどのような対策を取引先とやろうとしているのか、という点は個社のホームページを一つ一つ拝見しないと分からないという実態である。どの企業が、取引先とどのようなサイバーセキュリティの取り組みを実施しているのか、現状を把握したい。
- ・ セキュリティ対策の必要性を感じていない企業について、サイバー攻撃を中小企業でも受けている事例を継続的に発信していくことが必要である。事例の発掘については、例えばサイバーセキュリティ保険を扱っている保険会社にご協力いただくといった方法などを考えたい。
- ・ 中小企業に何かあった際の相談窓口の分かりやすさや体制整備は重要である。事故やインシデントが発生したときに、相談の受付時間が平日の昼間に限られており、必要な時に相談できないといった課題もある。どんなときでも対応していただけるような窓口があると良いのではないかな。これにはサイバーセキュリティお助け隊サービスが活用できる。
- ・ 発注側になる大企業としては取引先のセキュリティ対策状況を評価するにあたり、どこまで調査し、結果をどこまで取引条件にすべきか、という点が悩みとなっている。情報セキュリティに関しても取引契約する際のガイドラインを作ってはどうか。
- ・ 脆弱性評価も含めたチェックリストやそのガイドラインがあると運用しやすくなるのではないかな。
- ・ 専門性を有するセキュリティ担当者の現場での育成は困難で、それら人材はセキュリティベンダーや研究機関に採用されることが多くなっている。ユーザ企業でも専門性を有するセキュリティ人材を確保する必要性は認識されているが、評価や処遇等の面からそれが進まないという現状がある。こういった状況を打破するために、セキュリティ人材のシェアードサービスのような機関を検討することも一案である。
- ・ お助け隊サービスは、年間売上高の中央値より低い層をターゲットとみている。中央値より高い層へサービスとして適当かどうかという議論をしているが、対象企業を売上高だけではなく、業種、業態、重要インフラか否か、といった側面から対象となる中小企業を分けることを本WGで決めてはどうか。中小企業を分ける議論より、分けかたを決めて分析を進めたほうがよい。
- ・ 今後、労働人口が少なくなっていく中で、セキュリティ人材だけが増えるということはある得ない。業務を集約して人をかけないカタチとすることが必要であり、お助け隊サービスの次にくる必要なサービスを、国や産業界がこれを使いなさいという形で示していくことが必要で議論すべきではないかな。
- ・ セキュリティアクション等を充実していく、あるいはSC3でガイドラインを示していくことは非常に重要である。ガイドライン

だけではやりきれない部分をサポートする人材として、登録セキスペの活用が重要であり、登録セキスペが活躍できない理由を調査し、分析すべき。また、中小企業にどのようなサポートができるかといったひな型を用意した方が良い。中小企業もビジネスを拡大するためにセキュリティも対応するので、ビジネスとセキュリティのバランスをどのようにとるかといった、登録セキスペ向けのガイドラインをIPAから出してはどうか。

- ・プライバシーマークの黎明期では、地方公共団体が調達要件にしたことで個人情報の取り扱いの意識が高まった。セキュリティアクションの2つ星を宣言している会社と取引をすることを原則とする、などと発注側が宣言することにより、ビジネスと直結するため、受注側の中小企業が危機感を持って取り組むのではないか。
- ・地方の中小企業では、セキュリティに関する人材を雇いたいと思っても、そもそも人材がいない、給料が見合わず雇えないといった問題がある。セキュリティ意識を広げて裾野人材を広げるためには、地域DX促進活動支援事業のような取り組みをきっかけに活用することが有効。
- ・大学側もリカレント教育に取り組んでおり、文部科学省からの関連のさまざまな事業でもDXは必ずあるテーマとなっている。セキュリティについても、公募する際のテーマとして設定をすることにより、取り組みが広がるのではないか。
- ・中小企業への対策については、中小企業を分類し、それぞれにアプローチを変えないと進まない。分類には規模もあるが、業種によって経営者のマインド等、様々な違いがあることから、ある程度分類してそれぞれに通じる言葉で伝えることが重要である。
- ・この分類する作業はSC3等で実施することがふさわしいがなかなか議論が進まない。業種ごと規模ごとに対象の社数がそもそも何社あるのかなどベースとなる数値を押さえて、打ち手を決めるということ。大企業のグループの傘下などに入っているならば親会社に任せる、独立企業であればどうする、といった細かい話をしていくのが次のステップではないか。
- ・セキュリティ成熟度は、単にテクニカルな対策のレベルだけでなくビジネスの体制やレジリエンスがどれだけあるかという観点が評価されるとよい。
- ・法律を作るとまではいかなくとも何かしら義務という社会的なコンセンサスがとれるような仕掛けあって、それを超えてプラスする人を褒めましょうというカタチが自然なのだろうと思う。
- ・人材について、ユーザ企業においてセキュリティ人材と定義づけた人を教育したが、トップガンになりたかったのか、セキュリティのコンサルタント会社へ転職してしまった。ユーザ企業においては、日頃からインシデントが起きることもなく、地道な活動しか経験できないため、学んだ専門知識を活かせないといったことがあったのではないかと思う。教育の中身を変え、経営的なセンスと技術的なセンスの比率を変えた人材を育成すべきか、それともIT人材にプラスセキュリティするほうがよいか、といったことを考えている。
- ・中小企業の企業数は420万社以上あり、そこに対して今いただいているお題をまともにやることは不可能。不可能を可能にするには、インフルエンサーの起用や、メディアを積極的に利用することで理解促進を図るといった、ラストワンマイルのやり方をダイナミックに変える時期だと考えられる。
- ・発注側企業と取引先のパートナーシップについて、発注側企業が取引先に対して助言・支援をすることを求めているが、その対策例の記述が無く、受け取った側は自分でやらないといけないという受け止めになっている。何をやれば良いかという例示や具体策をマニュアルや例示でも良いので提供するという取り組みが必要ではないか。
- ・SC3については、会員にならずとも恩恵を受けるコミュニティレベルの仕組みがあれば拡大するだろう。
- ・セキュリティ対策を含めて情報システム部門のシェアサービスの活用の有効性について、公助という部分で経済産業省、IPA、JPCERT/CCが有用なツールを提示していただくと良い。海外の先行事例を参考にし、使用環境は基本的にスマートフォンである前提で、アウトプットの出し方も工夫を凝らしてはどうか。

- ・相談体制や被害状況の把握、被害の拡大防止については、中小企業410万社に対して、JPCERT/CCやIPAを合わせた100人程度で対応するのは不可能。これまでJPCERT/CCやIPAが手作業で返してきたレスポンスのデータが残っていれば、AIなどを使って一次受けができると思う。
- ・お助け隊や地域セキュリティといった仕組みは整ってきており、セキュリティに関心のない方々に、どのように関心を持っていただけるかということが、残る課題。一番インパクトがある対策は規制だと思う。
- ・法規制以外に何かできることはないかと言うと、メディアを巻き込んだ広報は効果があると思う。広報の力を積極的に借りていくべきなのではないか。経営者の方々が良くご覧になっている番組を中心に、隣が気になる日本人に向けて、お隣はこのような目に遭っている、このように動いているという話を差し込んでいくと良い。また、お助け隊サービスがありますよ、と落とし所まで出してあげると非常に良い。
- ・中小企業の人材不足と登録セキスペの活躍と拡充については、JICAの青年海外協力隊や総務省の地域おこし協力隊のように、年限を絞って2、3年ぐらい地域や中小企業に派遣するというやり方も考えられる。分析とあわせて、現職を辞めて参加し、2、3年地域で経験を積んで東京や各都市に戻ってきてまた改めて就業するということもありなのではないかと思う。
- ・プラスセキュリティ人材について、管理者を含めた現場の方々が、何が必要なかということを知らせておくが良い。
- ・中小企業サプライチェーンについては世界的にも同じ課題がある。日本だけが中小企業が多いわけではなくて、ドイツもアメリカもイギリスもフランスも中小企業は多いわけで、他国の中小企業に対する政策を確認してはどうか。
- ・サプライチェーンの対策について、法規制の議論を始めるタイミングかと思う。重要インフラ企業及びそのサプライチェーン関連の中小企業においては、一つの企業ではお金がないから対策しない、対策しないことが社会全体に多大な影響を与えるという可能性もあり、法規制の議論すべきタイミングだと考える。
- ・重要インフラ以外のサプライチェーンや中小企業については、サプライチェーンのトップ企業がサプライチェーン全体の対策を行うという方針を決めれば実施することになる。方針を受ける側の企業というのは複数社と取引しているので、ばらばらな事を言われても困るといった話もあるが、業界内の情報に大きな差は無いので、トップ企業が管理できる基盤を作り、取引企業に使わせるという形にすれば、大きなコンフリクトは生じない。
- ・人材に関する政策は普及活動が十分ではない。デジタルスキル標準を使って整備しているが、普及活動するのが重要である。
- ・社員が少数の中小企業ではサイバーセキュリティ担当を抱えられない。自動化やクラウドプラス、登録セキスペといった専門家をパートで雇うといったことが考えられ、中小企業がそれらに簡単にアクセスできるようにするのが良い。
- ・最初に就職した会社で社会人人生を終えるのではなく、セキュリティ業界の中でスキルを養い、様々な会社を渡り歩くことが当たり前になるような社会がセキュリティ業界の中にあっても良い。
- ・経営者が自社のセキュリティにどのように関与すべきか分かっていないので、経営課題として全社で取り組むことが重要。民間企業で経営者がCISOと協力して対応しているかレポートされており、これらを参照してイメージを膨らませてはどうか。
- ・メディアで取り上げられるサイバーセキュリティの話題は、ネガティブな内容が多い。サイバーセキュリティ人材は多くのインシデントを食い止め、インシデントに全力で対応している。セキュリティ人材、橋渡し人材、プラスセキュリティ人材がどのように日々戦い、努力しているのかにスポットライトが当たるよう、メディア関係者へ地道にアプローチすべき。
- ・最近ではサイバーセキュリティインシデントが増えているため、広報担当者もセキュリティについてある程度の理解が必要となっている。いざという時に備え、どのようなプレスリリースやメディア対応が求められるのかというノウハウを、サイバー演習を通じて広報や会社の中で溜めていく必要がある。

- ・最近、台湾有事の可能性が話題になっている。ウクライナ情勢から学んで、今からどのような準備をするべきなのか、本WGだけではなく、日本全体で議論が必要ではないか。
- ・地域の関係者との交流の中で、ラストワンマイルというキーワードが印象に残った。個人商店のような企業の場合、セキュリティの認識が薄いケースがある一方で、ライオンズクラブといった我々の知らないラストワンマイルの方々の取組がたくさん存在している。このような方々をどのようにサポートしていくのかということに大変興味を持った。
- ・建設業界ではDXを推進しており、この業界には10人以下の工務店が80万社程度いるが、DXから逸れていく工務店をどうするのか。数社をまとめてクラウド化やシェアードサービス、セキュリティ人材のシェアードのようなことも考えられるが、セキュリティに関する事項は信用のおける人間にしか任せられない、といった意見もある。様々な意見はあるが議論が必要。
- ・経済産業省へ戦略レベルでお願いしたいことを7つほど申し上げたい。
- ・1つ目、経済戦略として明確にサイバーセキュリティを位置付けていただきたい。大きな予算の中で骨太の政策を打ってほしい。全員を救うのではなく、ある程度優先順位をつける事が必要。
- ・2つ目、産業政策について、どこの業界を優先するかを決めた後に、業界毎や産業毎にリスクシナリオを作り、経済産業省の所管産業でなくてもリードを取っていただきたい。
- ・3つ目、国際戦略について、海外企業向けのお助け隊はないのか。日本にとって重要なサプライヤーに関しては、企業に任せるだけではなく、金銭的なものを含むサポートをした上で評価していく政策論があってもよいのではないか。
- ・4つ目、労働市場について、外国人がCISOやセキュリティマネージャを担当されている日本の企業もある。もっと門戸を開くと同時に、日本から海外にセキュリティ人材を輸出していくようなスケールで市場を考えていただきたい。
- ・5つ目、インセンティブについては税制優遇が一番効くが簡単ではない。例えば、警察と官民のテロ訓練のように、システミックリスクに対する訓練を日頃から実施しておくことも考えられる。知的財産に関しては、特許の承認を迅速化しインセンティブを与えており、インシデント報告が早い人への何等かの褒賞や緊急融資の保証等を与えてはどうか。
- ・6つ目、セキュリティ優良企業の評価について、リスク選考は企業の自由裁量なのでおまかせはできない。さじ加減を考える必要があり、功利主義的な倫理が良いのではないか。
- ・7つ目、バイヤーがサプライチェーンを管理するのは当たり前だと思うが、システミックリスクの場合には問題を特定し、官民で考えるべきものもある。特に国際法を含めた法対応は企業だけではできない。国際的なサプライチェーンに関しては、これまでと異なる見地から考えて頂きたい。
- ・サプライチェーンに関してはパートナーシップ宣言で対応すると考えられているが、欧米の企業では、サプライヤーとの契約を場合によっては解除しているので、必ずしもパートナーシップのモデルだけが正しいかはよくわからない。
- ・安全保障の問題とサイバーの問題について、大企業の中には台湾有事を想定したサプライチェーンのリスクのシミュレーションを本気で実施しているところもある。シミュレーションの結果から、最悪のシナリオとしてシステミックリスクがあり、別の場でサイバーを含めた議論をしたほうがよいと感じている。
- ・安全保障の問題について、問題認識が共通していると思うが具体的な方法論の議論は難しい。いまのセキュリティ意識の状況は非常にまずい状態だという認識を持つ必要があるのではないか。つまり、日米欧や新興国を含めて、日本がその中で特別に悪いわけではないが、セキュリティ対策をやっていないと答える人たちがいるのはまずい。それはセキュリティ対策を講じることが常識になっていないということ。ナショナルセキュリティを考えるにあたって、その意識を変えられないか。
- ・性善説で一つずつやる、DXにセキュリティも必要でDX優先でもよいといった進め方はまずいのではないか。ハードロ

ーで法規制をやれということ強い言葉で言ったが、それに限らず、何らかのカタチで人々の意識を変えて、せめて無免許運転しては駄目だという意識を持つ人が普通になって欲しい。

- ・自動運転などの議論のときに車がそもそも60km以上出せなくなれば、速度規制はいらないという話もある。スマートフォンも然るべきソフトがインストールされていなければ使えなくなるということの方が、ハードローよりも受け入れられるかと思う。
- ・サイバーセキュリティ経営の実効性の向上について、省庁が発行しているメールマガジンは相当な数がある。他の省庁から出しているメルマガに対して、経済産業省からセキュリティのテンプレートを渡し発出してもらおうといった取り組みがあれば、その情報を恒常的に確認できる利用者が多くなるのではないか。これはお金をかけなくとも政府内でできることであり、検討いただきたい。

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