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（地域・中小企業支援）（第11回）
議事要旨

1. 日時・場所

日時：令和7年4月15日（火） 10時00分～12時00分

場所：オンライン開催

2. 出席者

WG2委員　：梶浦委員（座長）、岩下委員、落合委員、小原委員、塚本委員、土佐委員、名和委員、原委員、藤本委員、藤原委員、丸山委員、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 奥家大臣官房審議官、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。

＜中小企業施策・サプライチェーン対策の強化について＞

- 事務局説明の内容は非常に重要なものと認識。法案等の国会審議や日本経済新聞へのサプライチェーン強化に向けたセキュリティ対策評価制度関係の記事掲載を始め、世の中の注目も浴びつつあると考えている。他方、これらが対処するサイバー脅威が世の中で蔓延しているという状況は決して望ましくない。
- 当社はサプライチェーン上の位置づけとしては主にサプライヤーにあたる。近年、海外の顧客からサイバーセキュリティ対策のレベルを細かく問われている。営業からは先方の求める水準に 1 ポイント足りないと言われる等、対応には苦慮している。日本でサプライチェーン対策評価制度★5 を持っているから OK ということを海外に向けても言えるようになればより活用が広がるのではないか。
- 評価制度はこれまで SECURITY ACTION しかなかったが、★3～★5 の取組は高く評価できる。基準ができればどこまでやってほしいか求める側も言いやすくなり、優越的地位の乱用などにも当たらないものと納得できる。サイバーセキュリティお助け隊サービスは商工会議所でも普及に向けて活動しているが、折角なので既存の施策と評価制度との連動を深められたい。中小企業と言っても千差万別で、サプライチェーンに組み込まれるような大きなものから家族経営の小さなものまであるため、サプライチェーンを構成する中小企業などである程度絞って取り組むことは重要。中小企業のリテラシー向上と言う観点では粘り強く長期的に PR していくことが必要である。
- サプライチェーンに組込まれるような中小企業の多くは製造業であり、品質を重視するので顧客が立ち入り検査するような取組は以前から行ってきたが、サイバーセキュリティの検査は考えることが多すぎてより困難である。品質とセキ

ュリティが同じくらい重要であると元請けから伝播させていく必要があると思料する。

- 日本情報システム・ユーザー協会(JUAS)では情報セキュリティ WG を設置しており、事業会社のセキュリティ担当の部課長クラスが参加している。マネジメントに関わる課題やインシデント発生時のソリューションをどのように構築していくのかを議論している。構成メンバーのほとんどは大企業関係者なのでセキュリティの理解度は高く、対策を実行されている企業が多い。関心が高いのはランサムウェアへの対応。インシデント発生時に備えた訓練（どのように意思決定をして、どのように対応していくのかというプロセス作成） ITDX 部門だけではなく、コンプライアンス部門含めて訓練されている企業が増えている。そのほかは、セキュリティ人材の確保等である。
- 今年度はサプライチェーンの関心が高くなっており、サプライチェーン対策評価制度への対応が大きな議論ポイントになってきている。中小企業について十分な情報はないが、サービスや製品を作るプロセスに組み込まれているならば、全体のレベルを上げていく必要がある。中小企業の経営者の意識の問題なのか、意識はあるがどこから手を付けてどこまでやればいいのかわからないのか、企業の本音を引き出して芯を食ったような取組が必要である。
- サイバーセキュリティ対策に関心のある方はセミナー等に参加するが、関心のない方にどうアプローチするかが大きな課題である。ソフトウェアで様々なサービスやプロダクトが作られている中で、サイバー空間でのセキュリティ確保の重要性をうまく伝播して国民全体できっちりと対応していくということを意識づけていくことが重要である。
- 先ほどから規制というワードが出ており、ある程度必要であるということは理解するものの、それらをチャンスだと経営者が思えるかが重要である。セキュリティがしっかりしたものを提供できるということはマーケットに対する訴求もあるはず。ビジネス上の価値を理解することが必要。制度対応が受け身にならないように対応したい。
- 昨年度に経団連の活動で訪英した際、Cyber Essentials という類似制度について紹介を受けた。第一段階は自社で手を上げるだけだが、第二段階は外部監査付きで何万社も取得したと言っていた。その際、取得件数ではなく、取得企業でどれだけ売上が上がったか等を KPI にすべきではないかと指摘したが、1 年かけて検討を進めていただいている模様である。日本でも同様の観点をもって取り組むとよい。
- サプライチェーン対策評価制度について、「求めよ、さらば与えられん」という段階まで来ている。ただ現状では求める企業の数がまだ足りないということで、認知度向上が課題である。テレビやラジオ等のメディアも活用されたい。地方ではラジオも有効。ラジオの視聴層は 40～69 歳で仕事中に流している方が多いと聞いている。地域密着のラジオ局とも連携されたい。地域 SECUNITY の皆様、お助け隊の皆様の地域ネットワークを使って訴求をすると、より認知度が上がっていくと思う。認知度向上については、Google が先日「Japan Cybersecurity Initiative」を設立したが積極的に連携してはどうか。
- 中小企業のサイバーセキュリティについて、国としてのサイバーハイジーンを上げるために効果的に取り組むことは重要である。
- 本日IIJから情報漏えいのニュースがあったが、これまで大丈夫だと思われていた重要インフラに関連する企業のサイバーセキュリティがそれほど万全でないという点について確信が高まりつつある。安全保障の問題ともかかわる非常に重要な点である。
- ランサムウェアやサプライチェーン攻撃が引き続き重要な位置づけとなっている中、中小企業の意識が余り高くなく、政府としてはアメの施策を中心に講じてきた。一方で、ムチにあたる強硬性のある施策を講じなければ普及が進まない点も社会的な認識になりつつあると考える。
- サイバーセキュリティは多くある社会的課題の一つであり、例えば火災対策や食品衛生等の領域では違反があった場合ペナルティが科される施策が講じられている。昨年は、火災で 600 億円程度、食品安全でも数十億円の経済被害が生じているとされているが、サイバーインシデントでは 1 件 500 億円を超えるものも起きており、社会に与える影響についてもそれらに匹敵するレベルになってきている。火災については建築基準法や消防法等、食品については食品衛生法等の規制法があり、対策を怠った場合に営業停止等のペナルティが与えられるが、サイバーセキュリティではそのような罰則は基本的に講じられていない。

- 被害がそれほど身近でないのは当たり前だが、火災や食中毒が身近では無いのと同じで、それを防ぐ必要があるという点では、伝統的なハザードに匹敵するものになってきている中で、深刻化すると国家規模の災害になり得る。インターネットをビジネスで活用することが一般的になっている中で、サプライチェーンセキュリティや入札要件のようなルールは出てきているが、甘いことを言っていられない時期に来ている。アメとムチの上手な使い分けは必要だが、どうやって隅々まで施策等を浸透させるか是非引き続き検討いただきたい。
- ウイルスソフトを導入していないことをもって罰則適用となると、調べ切れるかに課題があるが、サイバーセキュリティ対策状況を有価証券報告書等への記載を求める等、様々な施策が考えられ得る。
- 欧州などでは規制が非常に厳しくなっており、産業や分野によっては大きな罰則が科される。これらは過剰なのではないかという議論は存在する。過剰な規制がゆえに萎縮ではないが、問題が複雑化している傾向もある。対策が細部にわたりすぎて足をすくわれるケースもある。本末転倒にならないよう、理屈だけでは限界がある点を認識する必要がある。
- サイバーセキュリティ対策を”Nice to have”から Mandatory に移行していくのがよいのではないかという観点から複数コメントしたい。
- 当方が日頃お付合いのあるのは中堅企業や中規模の自治体関係者が多い。環境や人権デューデリジェンスについては報告や第三者による検査をしなければ取引が継続できなくなるため対応が優先されるが、情報セキュリティはそこまでの要求水準ではないため後回しになる傾向がある。”Nice to have” から少しレベルを上げるとよいのではないか。
- 先月日本サイバーセキュリティ・イノベーション委員会(JCIC)の会合でサイバーセキュリティ基本法の施行から 10 年ということでディスカッションを行った。10 年前の認識が薄かった状況からすると大企業の意識は大きく変わったと多くの方が感じており、暗黒の時代からスポットライトを浴びる時代となった。その意味で、深刻さに十分気づいていない中小企業への対応の重要性が高まってきたことと理解。その差をどれだけ埋められるかが肝。アメとムチも使って、わかりやすい言葉で、認知度を高める必要があると認識している。
- 業務としてペネトレーションテスト、フォレンジック、インシデントレスポンスの支援を行っており、インシデントの現場に行くことが多い。インシデントが発生してから、国会議員、行政機関、研究機関、元請けなどの発言や姿勢を見ると、(現場との)心が離れていっているようにも感じる。現場の話を聞くと国会議員や行政機関などは俯瞰的知見が強くて、現場の実情を十数年以上アップデートされていないと感じる。
- 基幹インフラの方でインシデント対応に 3～4 日かかると立腹されるケースがある。現場の状況を聞くと、特殊法人や行政機関を含めて形式的評価の期待が強すぎると感じている。現場で見つかる脆弱性への対処について解決すべきと助言しても、これは都合が悪いからとか予算がないかとか、あとは上層部に過去の施策や取組を否定することは言えないので、実情から離れた表現をされてしまうことがあるが、半年以内に深刻な被害を受けるケースもある。
- 迅速な現場介入、意思決定の歪みが最近著しく、対応における法務、コンプラ部門の位置づけが強くなっている。知識不足により意思決定プロセスが稚拙になっており、解決するには上層部を入れ替えるか、現場を勉強してもらうしかない。
- 調査や診断の事業費用と事前見積もりのギャップがひどく、フォレンジック等で追加費用が掛かるというと強く反発されて実施しなかったことがあるが、結果として被害が継続したりするケースがある。それら現場の実態を国会議員や行政機関が承知していないケースがあり、施策検討時にしっかり了解しておいてほしい。
- これまでに引き続き東京商工会議所が会員企業に対してサイバーセキュリティに関する調査を行った結果を見ると、対策はほぼ 8 割の会員企業で実施していると回答。一方で中身を問うと、ウイルス対策ソフトの導入・アップデートが 7～8 割を超えている一方で、ファイアウォールの構築や従業員教育などになると 2～3 割に落ちる。それらが中小企業の実態になる。経営者の意識はある程度重要であり、ベンダー任せになっているところもあるが、まじめにやろうとしている経営者も何をどこまでやっていいかわからない状況になっている可能性がある。

- 他の委員から意見があったが、経営者の能力についても意見したい。当方が業務上関わりのある企業は能力の高い経営者であることが多いが、海外の方と話をすると、海外の企業に比べると日本の企業では、サイバーの知識や経験が不十分な方が CISO になっていると驚かれる。また、マネジメント能力の欠如も指摘されており、過去のルールを無批判に踏襲するなど、現場が経営側に忖度しているのを放置している面もあるのではないか。チェックリストをつぶせば OK という形式主義が蔓延してくると良くないと思う。こういったことは結果的に、今後の日本の発展の足かせとなり得る。
- 他の委員が指摘したように、最終的には経営者を変えなければならない。投資家や取締役、監査役など、ガバナンス全体の問題として議論しなければならない。スチュワードシップやコーポレートガバナンスコード等、以前から取り組まれてきたことをさらに深化させ、投資家も含めてサイバーセキュリティリスクに対するより深い理解を求めるべき。
- また、国会議員等に対しても適切なインプットを継続的に実施していくことが重要であると感じている。正しい知識を適切な人に届けていくという意味で、普及啓発活動を優先度を高くして実施する必要がある。
- 他の委員の意見にも関連するが、会社の経営層にセキュリティの重要性を理解いただく必要がある。最近になり、企業との接点も増えているが、経営層にそこまで高い能力はいらない。詳細なサイバーセキュリティの知識は必要なく、大事なテーマだと分かっていただく程度でよい。残念ながら、日本企業は、上場企業の取締役のリスクマトリックスでサイバーセキュリティやデジタル、イノベーションと記載のある企業はほとんどないが、重要性はある程度認識してもらいつつあり、それを担う人材もいると思う。サイバーセキュリティの専門の大学院を出た人間でなければいけないという話ではなく、通常の理解と能力があればできるという話に持って行くべきだと思っている。
- 海外と日本で差が出ているのは、求めているレベルが異なるからではないか。スマホや PC を毎日使っている人はある程度セキュリティを理解していると思う。きちんとした制度的枠組があった方が実効性を持つ形で進められるのではないか。
- FUD(Fully Un-Detectable)という略語がある。セキュリティの分野では、完全に検知不能という意味だが、マーケットを見ている方々からするとFUD(Fear(恐怖)、Uncertainty(不確実性)、Doubt(疑念))がもたらすリスクということになる。
- 経済産業省はじめ関係省庁が真剣に長年議論されていることは大変なことと思う一方で、精緻化が進み過ぎている部分がある可能性もある。つかみで何を言っているかがわかるような発信も重要ではないか。また、親会の存在意義をもう少し社会に知っていただくことが重要ではないか。具体的に、サプライチェーンの本質は価値がつながり、増大することにあるが、サプライヤーがサイバーセキュリティ対策をするとサプライチェーンの価値は増すはずである。
- 品質管理、納期管理のレベルが上がっていることに着目すると、サイバーセキュリティ管理をしっかりしている会社に対しては購買単価を上げるというメッセージを出すと非常に伝わりやすいのではないか。お助け隊のサービス、サイバーリソースの問題も徐々に解決していくと思う。新入社員の給料を上げるだけでなく、理由を明確に、購買単価を上げることが大事。その裏には、サイバーセキュリティ対策は経済合理性の中で行うものであって、倫理等の問題ではない。セキュリティ原理主義に陥ってはいけない。
- 先ほど申し上げた、過度の精緻化の弊害について、これを除去するための政策を検討してはどうか。一案としては、国内にあるサイバーセキュリティ対策関連の諸団体が多すぎることの悪影響を排除するため、合従連衡の旗振りを行ってはどうか。
- 中堅・中小を含む委託先やグループ会社でのインシデントを防ぐために色々な手段で手を打つ必要があるが、そのコストをどう負担するか、ある程度のレベルを求めると各社や海外現地法人で負担してもらわないといけないという税務上の話が出てくる。利益供与に係る税務上の問題が解決されておらず、親会社に予算や人材があったとしてもそこに投入できないもどかしさが続いている。また一方、サプライヤーの立場では中堅・中小を含む顧客に対してサイバーセキュリティ対策に手を差し伸べることに躊躇せざるを得ない。大手が中堅・中小企業に手を差し伸べられる制度として取り組みやすくなるよう配慮していただけるとありがたい。民間の立場だと一般的には規制をかけないでくれということになるが、サイバーセキュリティに関しては、何か明確なルールがないとこのままでは限界が見えている。

- 以前から指摘されている税務上の利益供与の問題、取引関係における優越的地位の濫用の問題があるが、後者については公正取引委員会と経済産業省の共同文書が出ているが、浸透はこれからという印象である。前者は国税庁などからの文書等は特になく、目立った進展はない認識である。
- 税務上の利益供与の問題については、管理会計と財務会計を分ければ解決するのではないか。付け替えを管理会計で行えば大きな問題にはならないのではないか。
- 中小企業からのサイバー保険金請求は増加傾向にあるが、保険に入っている中小企業は全体からみると微々たるものである。サイバーセキュリティに対してアンテナの高い企業が保険に加入しているが、そういった会社でもサイバー攻撃等による被害を受けている実態がある。ランサムウェアのような深刻なものもあるが、頻繁に起きているのはテクニカルサポート詐欺、SNSアカウントの乗っ取り、不正なメールのバラマキ等である。それらを通じてパソコン内部への侵入を許しているわけであり、攻撃者のレベルが高い場合はより深刻な被害が起き得ると心配している。今回説明のあった施策は啓発や指標と言ったサイバーセキュリティ施策であるので、まだサイバーセキュリティに興味を持たれていない層に対し、気付きを与える施策となるとありがたい。
- サイバー保険の話で言うと、これまではフォレンジック費用や被害者へのお詫びの費用など、事故対応に係る直接費用の請求が多かったが、最近は取引先から損害賠償請求を受けたという趣旨の請求が増えている。何が起きているかというと、サプライチェーンの中で影響が生じた複数の被害者に対する損害賠償が、事故を起こした会社に対して発生すると言う事例が増えてきているので、最近のトピックとして共有したい。
- 社内では IT-BCP の策定を進めている。最初の何日間かは全システムが停止し、全面復旧するのに相当の期間を要する、という想定で、ビジネスが止まらないような対応策の策定を各部へ依頼している。システムがなければ業務が継続できない、システムがなくてもある程度業務継続が可能などいろいろな回答があり、サプライチェーンを守るという観点で BCP にも大きな関心がある。

＜人材育成について＞

- 登録セキスペについて、情報システム部門の人がアテンションするかというと”Nice to have”だったり、日本では採用できないので、インドで CISM(Certified Information Security Manager)を採用した話を聞いている。国内で地位を上げたいのであれば、サイバーセキュリティお助け隊と絡めたり、必ず登録セキスペの助言を受ける等、制度間の連携を進めてはどうか。
- 登録セキスペの有効活用については、登録セキスペでしかできない業務を作り出さねば普及は進まないのではないか。ある程度の要員を抱えていると有価証券報告書に記載できるとか、システム監査のある部分が免除される等のメリットのある仕組みを作らねばならない。また、例えば取引先へのアンケート等の対応に人が足りないのだとしたら、登録セキスペに委託できる等の能動的な取組にも期待したい。
- セキュリティ人材について米国、豪州で 9 割が充足、日本では 9 割が不足と回答されているが、どうしてそうなっているか海外事例を今後さらに検討していく必要がある。国際情勢の変化の中で、サイバー人材は技術だけでなく、経営、国際情勢を含めて知見を得ておく必要性が高まっている。サイバーセキュリティに連なる企業に噛み砕いて分かりやすくお伝えしていくこと、独立した企業に行政から伝えていくことも必要と思っている。JCIC としては国際情勢にアンテナを伸ばすことを促すなどして、サイバーセキュリティを支える裾野を広げるという観点で、プラスセキュリティ人材の必要性について議論を続けている。初心者に寄り添えるという意味で地域でもプラスセキュリティ人材の活用が有用ではないか。
- セキュリティ人材を見える化し、活用できるような制度設計に期待したい。

＜国際連携について＞

- 主に大企業がメンバーであるリスクコミュニティの方々20 名程度と意見交換を行ったが、①セキュリティの領域が拡大

していて、例えば AI のセキュリティガバナンスなど様々な仕事があり大変であるという点、②まだまだだと思ったのが多要素認証、敵が社内にもいるという前提で多要素認証は必須となっているところ、利便性の関係から対策を解除してしまう事例があるという点が印象的だった。

- セキュリティ対策を担当している中小企業の方と直接の接点はないが、大企業がこういう状況だと、サプライチェーンの状況に目が向いて、手厚い対応が進むか懸念している。ただ、経済産業省や SC3 がセキュリティをサポートし、国がすべて面倒を見るわけでも、民間のように自己責任として厳罰主義にするでもなく、中庸な方法として全体の底上げを図る方法はよいものと感じる。ASEAN への発信においては、社会的・経済的な取組として推進しているという説明をすべきと考えており、カウンターパートもセキュリティ関係者だけでなく、政治関係の方も含めるとよい。
- ASEAN との連携について、域内にはシンガポールのような先進的な地域もある。ASEAN 向け企業対策支援について、支援や教えるという Give の観点ではわかるが、進んでいるものを取り込むという Take 観点の取組はあるか。日本のガイドラインをベースに ASEAN ガイドライン等を策定されると域内での認知度や利用度が高まるのではないか。
- 昔と異なり全部日本が優位というわけではなく、ASEAN からも学ぶべきものがあるということで理解した。
- 今年、米国では新政権が発足、国際情勢が大きく変化している。米国の同盟国・同志国との関係が変化しつつあり、米国連邦政府は CISA を含め予算・人員の削減を進めているようである。国際社会における米国のプレゼンスは今後大きく変わるであろう。激動の時代に合わせ、日本はインド太平洋での国際連携をどう変えていくつもりなのかご教示いただきたい。また、米国が非常に速いスピードで変化していく中、日本の情報発信も如何に対応していくのかについて教えていただきたい。
- 今後景気後退が進んでしまえば、残念ながら、中小企業がサイバーセキュリティ対策に目を向けられなくなる恐れもあるだろう。そのような場合に備え、国としてどう取り組んでいくのか。
- P.50 の＜国際連携＞における論点 2 について、経済産業省が作った貴重なガイドラインなので、日本企業が日本語で読んだり、英語でサプライヤーに提供したりすると大きな成果が得られると思っている。選択と集中の観点から、連携先として ASEAN 地域における日本企業主導の主要工業団地を扱っては如何か。

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