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12回）
議事録

1. 日時・場所

日時：令和8年3月3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　　：梶浦座長（座長）、岩下委員、落合委員、小原委員、武智委員、塚本委員、坂田様(土佐委員代理)、名和委員、原委員、藤本委員、藤原委員、丸山委員、湯淺委員、谷口様(横浜委員代理)

オブザーバー　：内閣官房 国家サイバー統括室、警察庁、総務省、厚生労働省、デジタル庁、独立行政法人情報処理推進機構

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、他

3. 配付資料

資料1 議事次第・配布資料一覧

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。

＜中小企業に対する SCS 評価制度の活用促進のために実施する施策＞

- 中小企業は、守るべき存在であるという前提で政策が立案されがちだが、情報セキュリティの観点では、企業規模に関係なく同一のインターネットを使い、同一のサプライチェーンに組み込まれている以上、情報セキュリティのリスクは同一で、セキュリティ対策が弱くてもいいという理由にはならない。かつては、情報セキュリティが、大企業や金融機関などのブランド向上のための投資という、一種の贅沢品のようなイメージがあったが、その感覚が依然として残っているのではないか。
- SCS 評価制度の要求事項・評価基準は、中小企業にとって最低限達成すべき必須の基準であるということを認識いただくべき。啓発だけではなく、ルール化する方向の議論を進め、最低水準に迅速に到達させるスピード感のある制度設計が必要。
- コーポレートガバナンス・コードについて、金融安定理事会において気候関連財務情報開示タスクフォースが設置されたのを皮切りに各企業で SDGs バッジを取得するようになったという事例もある。各企業に情報開示として、スキルマトリクスのような形でサイバーセキュリティに関する対策状況をアピールさせるのも良いのではないかと感じた。
- 多くの企業が実装段階で“国家最高機密レベルの完全防御”を理想に掲げ、費用不足でセキュリティ対策を断念しているように思う。セキュリティ対策においては、リスクをゼロにすることを目指すのではなく、あくまでリスクに応じた企業ごとの適切な対応を行うべきであると考えている。重要インフラ事業者から一般消費者に至るまで求められるセキュリティ対策のレベルは様々である中、レベル感が曖昧となっているため、最低限目指すべき基準が必要であり、高度なセキュリティ対策と最低限行うべきセキュリティ対策が混同している状況を整理した方が良いのではないか。この意味においては、SCS 評価制度の★3・★4・★5 のレベル分けは、市場にとって良いヒントになると思う。

- 具体的な業務レベルにおけるセキュリティ対策はリスクに応じて変化するため、企業のセキュリティを評価する際は、リスクを取り巻く変化に対応できるか、あるいはそれに対してリソースを配分できるマネジメント体制があるか、といったいわゆる ISMS のような評価軸がグローバルスタンダードになっている。日本国内でも JIPDEC(一般財団法人日本情報経済社会推進協会)が運営する ISMS 適合性評価制度が存在する。
- リソースが限られている中小企業では、セキュリティ対策に関する善管注意義務の責任分界点が不明瞭であることが課題になっており、SCS 評価制度における要求事項・評価基準、サイバーセキュリティお助け隊サービス(新類型)、情報処理安全確保支援士による助言は一つの解になると期待している。
- ISMS との関係は、資料では★5 で整理するものとされているが、★3・★4 においても関係の整理が必要。ISMS 認証を既に取得している真面目に取り組んできた中小企業が報われない懸念がある。
- ISO/IEC 42001 に基づいた AIMS 適合性評価制度が JIPDEC で開始されている。ISO/IEC 42001 では、AI に関する様々なリスクに関する要求が規定されているが、その中にはサイバーセキュリティに関する要求も含まれている。AIMS 適合性評価制度の取得を通じて AI に関連したセキュリティ対策に力を入れている企業も出てきているため、サイバーセキュリティの分野としても AIMS 適合性評価制度を支援するような政策があっても良いのではないか。
- サプライチェーンには多数の企業が関わっているが、サプライチェーン全体を見ている最終バイヤーが最終判断をするのが実態。最終バイヤーが脅威の見極めを行い、★3・★4 の区分を検討することが出発点ではないか。
- 例えば、ゲノム情報を扱っている企業に求められるセキュリティレベルが高いことは当該企業にとって自明だが、一方で最終製品のことを意識せずに部品を生産している会社からは、サプライチェーンの全体像は知りようがない。今回は中小企業のセキュリティ対策に関する議論を行ってきたが、大企業のサプライチェーン対策と絡めたうえで議論すべきではないか。
- BRICs・ASEAN・グローバルサウス・米国が世界の GDP の8割を占めている。サイバーセキュリティ政策の観点でも、国際競争力をメルクマールとすることが必要であり、グローバルな視点で見てどういう位置づけかという視点は重要である。
- 産業サイバーセキュリティ研究会は 2017 年から活動していることからも、研究会で議論された政策について、効果検証が必要であり、その効果が十分でなければ見直しをするべき。
- 産業サイバーセキュリティ研究会で議論されている政策は、産業振興のためにやっているという出発点を確認したい。今回の会議ではサプライチェーン全体のサイバーセキュリティ強化を中心に議論しているが、それが日本全体として産業振興に結び付いているかが重要。経済産業省では、結果の平等に焦点を当ててサイバーセキュリティ施策を立案しているが、結果の平等より、機会の平等に軸足を傾けても良いと考えている。全てのサプライチェーン構成企業にメリットがあるのは理想だが、それが現実的ではないとすると、メリハリをつけた政策が必要ではないか。
- 経済産業省貿易経済安全保障局経済安全保障政策課が 2026 年 1 月 23 日に公表した「経済安全保障経営ガイドライン(第 1 版)」は、国際競争で勝つためのヒントを記載した示唆に富む資料である。当該資料では、「自律性」及び「不可欠性」が政策のドライバーとして示されているが、これはサイバーセキュリティ政策も同様でないかと考えている。すなわち、サイバーセキュリティ政策における「自律性」は SCS 評価制度そのものであり、一方で「不可欠性」とは、国家の経済安全保障の目線に合わせ特定の技術や事業領域に注力するようなメリハリのある政策である。
- 我が国としてサイバーセキュリティを通じて経済的な成長やメリットを追求していくべきである。絶え間なくイノベーションを創出し、かつ自社の重要な資産をリスクから守ることで、自社の製品や技術、サービスなどが取引先を含む国際社会にとって不可欠になるという趣旨が「経済安全保障経営ガイドライン(第 1 版)」において記述されているが、これはまさに産業サイバーセキュリティ政策の目指すところだと考えている。
- SCS 評価制度は企業を評価する制度ではなく、我が国のサプライチェーンのレジリエンスを段階的に引き上げるためのレール設計である。本制度に対応できない中小企業が出る可能性も踏まえ、制度の妥当性・持続可能性につ

いて具体的に解像度を上げて議論し、2027 年 3 月の制度開始に向け、企業現場の実態も考慮して検討を進めるべき。

- 自社のリスクをどう判断するかは、最終的には経営の判断であるため、SCS 評価制度については、技術的要素と経営判断の要素の両方が含まれているのではないか。
- SCS 評価制度の★3 は、OT 領域は対象外となっており、これで何かを保証するのは難しく、大企業でも取得を促すことが困難という意見も出ている。個人としては、★3 は最低限のセキュリティを自ら管理できるという事を示す、入口レベルと認識している。一方で★4 は、自社の責任でセキュリティリスクを判断して対外的に説明できる体制があるということを第三者が確認するというレベルではないかと考えている。つまり、★3 と★4 の違いは、対策項目の量の差ではなく、引き受ける判断と責任の違いではないか。特に★3 は、セキュリティを自分事として捉えていない経営者にとっての入口になるのではないか。技術的対策のレベルを保証するのは難しい側面があるので、むしろ SCS 評価制度は経営者のセキュリティに対するコミットメントを世間一般に示す指標だと考えている。
- 2026 年 2 月末に公表されたコーポレートガバナンス・コードの改定案を見ると、「原則 4－3. 取締役会の役割・責務」において、サイバーセキュリティ、経済安全保障、地政学などに関する全社的なリスクの低減について言及されており、良い方向であると感じている。社外取締役が SCS 評価制度を確認ポイントとして紹介するのが良い。これにより各企業の意識向上が期待される。
- SCS 評価制度については相互認証を含めた海外展開を検討し、海外でも認知・通用する制度にするべき。現在では、地方大学等でも海外の連携先から国際的に認知されているセキュリティの対策を求められる。海外の顧客から認められる制度であれば、発注企業・中小企業・地方大学にとっても使いやすい。
- SCS 評価制度の★3 は難しいとの印象もあるが、要求事項・評価基準は当然取り組むべき内容。一気に達成するのではなく“物差し”として活用し、段階的に成長が分かる仕組みになるとよいのではないか。また、この要求事項・評価基準については、BCP の要素も今後考慮していく必要があるのではないか。
- 発注企業の立場としても、グローバルで事業を展開している企業が多くあるため、SCS 評価制度が海外の顧客からも認めてもらえるようになるとよいのではないか。
- SCS 評価制度の★3 のではセキュリティ専門家による確認を経た自己評価を実施することとなっているが、人間が確認を実施する以上、どうしても品質のばらつきが発生してしまうことが懸念される。加えて、各取得希望組織において確認を受けるに当たっての証跡の整備が一定程度負担になることも、制度普及を妨げる要因の一つになると考えている。ついては、各取得希望組織で★を取得するに当たっての最低限の証跡のセットを設定して、それを活用してセキュリティ専門家向けのケース演習など実施することを提案したい。FedRAMP 2.0（審査従事者教育・指導要領公開）では、審査従事者（3PAO の担当者）に対する教育を年間 24 時間実施することとなっており、その指導要領も公開されているため参考になる。
- 価格転嫁について、要請文・見積科目・合意記録のテンプレート化により、発注側・受注側の交渉負担を軽減できるのではないか。
- SCS 評価制度の★3・★4 を取得するために何をしたらよいかという相談を中小企業から受けるが、中小企業が★3・★4 を取得するのは難しいというのが率直な印象である。制度運用開始前後に、★3・★4 を取得するために中小企業が何をすべきかについて説明会等の開催が必要ではないか。
- サイバーセキュリティお助け隊サービス（新類型）には期待している。一方で、中小企業はサイバーセキュリティをコストと捉える傾向にあり、新類型の費用は既存のサイバーセキュリティお助け隊サービスの費用よりは高額になると思うが、投資効果を考えると決して高額ではない旨を伝えていく必要がある。
- また、中小企業が一方的なコスト負担を感じないようにセキュリティ対策にかかる費用を価格転嫁できる取組も重要である。今般経済産業省と公正取引委員会が共同で「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構築促進に向けた想定事例及び解説」を発出したが、このような取組は非常に重要なので、引き続き進めていただきたい。

- 中小企業にとって、サイバー攻撃の事案は報道ではよく目にするが大企業中心であり、自分事として捉えにくい側面があるため、「中小企業のための実例で学ぶサイバーセキュリティリスク事例集」は経営者にとって大きなきっかけとなる。
- SCS 評価制度を共通の物差しとしてサイバーセキュリティ政策を進めていくことは心強い。本制度の普及にあたっては、サイバーセキュリティお助け隊サービス（新類型）との有機的連携が鍵。新類型のサービスに対して期待しているが、サービスに関しては単に技術的サポートだけではなく、経営層に訴求できるような人材の育成も並行して進めていってほしい。
- SCS 評価制度が共通言語として機能するためには、★3・★4 を目指す際のコストを透明化し予見可能性を高め、税制優遇や集団的防御プラットフォームのような共同利用型のセキュリティ対策導入を検討することが重要。
- SCS 評価制度への対応に当たって各企業が何から着手すべきか迷わないために、各種ガイドラインをシナリオベースで再整理していただきたい。
- SCS 評価制度は経営者のセキュリティに対するコミットメントを世間一般に示す指標であるという意見があったが、どちらかというと SECURITY ACTION がその役割を担っており、SCS 評価制度は技術的観点が強いのではないかと考えている。
- SCS 評価制度における相互認証などの国家間連携も非常に重要だと考えている。多くの企業がグローバルに事業を展開している中で、海外事業に対するメリットとして、国家間での相互認証が必要と考えているため、ぜひ進めてほしい。
- 中小企業のサプライチェーン対策に当たって前提となる考え方は、サプライチェーンはネットワーク上に無数に広がっており、我が国の経済はそうした中小企業のネットワークの上に成り立っているのにも関わらず、中小企業のセキュリティ対策が不十分であるために、全体のサイバーレジリエンスが高まっていかないというのが根底にあると理解している。その意味では、個々の企業のみならず社会全体の問題であるという観点から、セキュリティに関してもう少し公助の視点も取り入れてもよいのではないか。
- SCS 評価制度の活用について、★3・★4 を例えば従業員 100 名規模の企業に取得を求めた場合、ハードルが高いのではないか。今後★5 について検討を進める予定となっているが、それよりも★3 の前提として SECURTY ACTION 二つ星を再度整理して★3 につなげる土台を形作った方が良いのではないか。また、SCS 評価制度に関して、確認対象となる証跡リストを例示するのは良いことだと考えている。
- SCS 評価制度は企業を評価するものではないという意見があったが、一方で制度名称のとおり、★3・★4 を取得している企業は、それぞれ一定のセキュリティ水準を満たしていると理解されるのが自然である。したがって、おのずと評価制度への信頼性が問われることになると考えられる。制度では自己申告をベースに評価するが、場合によっては虚偽の申告もあり得る。そのような場合に、例えば★4 から★3 に降格となるのか、あるいは★自体を取り消すのかについて予め整理しておかないと、制度としての信頼性が低下するのではないかと懸念している。
- ★3・★4 の取得に当たっては、経済産業省が許認可したものであると誤解されるおそれもあるため、SCS 評価制度は何かを保証する制度ではないことを併せて理解してもらう必要がある。
- SCS 評価制度と海外基準との整合性を確保することは重要と考える。大企業のサプライチェーン内で、様々なセキュリティ基準を要求されている企業が SCS 評価制度による基準の統一により、負担軽減になるという側面はある一方で、今日ではサプライチェーンが海外に存在する企業も多く存在すると思われ、国内基準と海外基準に整合性が無ければ単純に似たような二つの異なる基準に合致させる労力を求めることになる。そのような企業の取扱いについても、もう少し議論を充実させる必要がある。

- 地方でのサイバーセキュリティの仕事の少なさが人材育成の課題であるため、サイバーセキュリティお助け隊サービス（新類型）の担い手に地方 IT 企業も参加できるようにするべき。
- 海外とのサプライチェーンは、全ての企業に存在し得るため、国内で完結するものではないと考えている。SCS 評価制度と海外制度との相互承認も検討すべきである。
- 一つの企業が複数のサプライチェーンに関わっているのが実態であるところ、経済産業省には幅広い意見を募りながら今後の制度設計を進めていただきたい。
- SCS 評価制度は技術的指標に加えて、セキュリティに対する経営のスタンスを測る指標であると考えている。
- AI のような高度な分野はさておき、各企業で最低限のセキュリティ対策は実施する必要があるのではないか。これまで、弱い立場の中小企業をどのように守るかという視点で議論されていたが、中小企業であっても社会の構成員としてやるべきセキュリティ対策は最低限実施していただくという観点も必要ではないか。

＜地域 SECUNITY 活性化に向けて実施すべき施策＞

- 東北地方ではセキュリティ対策に係る活動が活発でないとの事例も紹介されたところ、セキュリティを自分事として捉えていない企業は一定数存在する。最近の事例を見ると、ランサムウェア被害を受けてサプライチェーンから外れると事業継続に関わる事態となり得るため、より危機感を促す政策が必要。
- セキュリティに関心のない層に政策やメッセージが届いていないのが課題。そのような層に届けやすい権威のあるチャネルを経由して連絡するのがよく、その意味では地域 SECUNITY は非常に良い枠組みであり期待している。
- 人口比で見たときに、都道府県ごとに IT 業界の従事者数や大学における情報系・コンピュータ系の学部の設置有無など、実情はさまざまである。地方への政策を検討するに当たっては、都道府県単位で細かく分析を実施することで、地域ごとの具体的な対策が見えてくる可能性がある。
- 中小企業の 8 割程度が対策を実施しているが、多くはウイルス対策ソフトの導入程度で、人材育成には手が回っていない。また、東北地方でセキュリティ対策に係る活動が活発ではないという事例の紹介もあったが、地方は首都圏に比べてセキュリティ対策が進んでいないのは否めない。粘り強く何度でも対策を促すことが重要。
- サイバーセキュリティに関心の無い層へのアプローチと地域ごとの人材格差の是正が必要であり、例えば地方のセキュリティ団体の連携や TIPS 集の公開が有効と考える。
- セキュリティにおける地域格差の壁をどう乗り越えるかについて、「中小企業向けサイバーセキュリティ対策支援者リスト」や DX 政策との連動を通じて情報処理安全確保支援士の社会的地位も向上してきていると思うが、依然として地方を中心に人材不足となっている。
- 中小企業における人材確保は難しいため、都市部の情報処理安全確保支援士が副業・遠隔サポートで地方企業を支援できる仕組みが必要であるが、受け入れ側のマインドセット改革も必要。こういった人材プールの循環を促す取組をぜひ検討いただきたい。
- 2017 年から本ワーキンググループにて議論しているが、サイバーセキュリティの危険性に気付いている人には必要十分な政策が届いているという、まさに「求めよ、さらば与えられん」の段階にきていると感じている。残される課題は、「求める必要があること」を認識していない層へのラストワンマイルの政策。
- 地域 SECUNITY 連絡会は政策として好事例であり、海外にも展開してよいのではないか。
- 昨今のサイバー攻撃事案の影響もあり、日本全国の経営者においても、自分の会社は大丈夫なのかという危機感がある状態。この危機感を踏まえ、サイバーセキュリティ対策の必要性を各経営者に打ち込んでいく良いタイミングではないか。
- 商工会議所、地方金融機関、ロータリークラブなど地方の経営者を束ねる組織と連携し、さらに一層メッセージを打ち出すべき。

- 東京で立案された政策は、地方企業の実情を理解していないのではないかという地方の企業におけるフラストレーションがあるのではないか。地方への支援を検討するに当たっては、政府の政策を地方に伝播するというスタンスになりがちだが、まずは政策の対象者の実情を的確に把握していただきたい。
- 机上演習はセキュリティ意識を高めるためには、非常に有効な方法である。一方で、こうした演習で最も重要な要素はファシリテーターであると考えている。ファシリテーター研修などを充実させたうえで、情報処理安全確保支援士にファシリテーターを担当していただくのが良いのではないか。
- 地域 SECUNITY ついて、地方からは、地方の実情について東京にいる我々の理解が足りていないのではないかという意見がよく聞かれる。地方のために良かれと思って進めている政策が必ずしもそうではないということもあるのではないか。地方局では経済産業省と総務省が連携して政策を進めているイメージもあるが、一方でサイバー犯罪に関して警察も力を入れて取組を進めている。警察の活動に対して総務省・経済産業省が連携していくことが重要。
- 地方においては、地方銀行とも連携して企業のセキュリティ対策を進めていくことで、結果的に銀行としても与信リスクが減ることになるため、有効ではないか。
- 情報処理安全確保支援士の地方での普及は重要である。地方でのセキュリティの仕事がないというのが課題になっているため、SCS 評価制度やサイバーセキュリティお助け隊サービス、また他の委員から提案のあった机上演習のファシリテーターなども含めて、活用を進めていくことで、情報処理安全確保支援士のプレゼンス向上につながるのではないか。
- 地域 SECUNITY について、人口比で見たときに、都道府県ごとに IT 業界の従事者数や大学における情報系・コンピュータ系の学部の設置有無など、実情はさまざまである。地方への政策を検討するに当たっては、都道府県単位で細かく分析を実施することで、地域ごとの具体的な対策が見えてくる可能性がある。
- 現状は経営者側の意識は高まっているものの、その高い意識を現場に落とすところまで理解が進んでいないものと思われる。各経営者の意識が高い今こそセキュリティ対策の必要性を感じてもらうべきではないか。サイバーセキュリティは投資であるという必要性を理解してもらうためにも、経営層への働きかけを不断なく進めてほしい。

＜中小企業のセキュリティ対策底上げのため更に実施すべき施策＞

- セキュリティ対策の課題は、体制整備の猶予を求めても、攻撃者は待ってくれないという点である。国会も含めてサイバーセキュリティについて議論になっているとのことだが、アリバイ作りのようなものではなく、即効性や実効性のある政策を進めていただきたいと考える。
- セキュリティに関しては、ISMS や P マークなど、認証制度の先例は存在している。一方で、認証取得によるセキュリティに関する免罪符を求めてしまい、実効的なセキュリティ対策につながらないという課題もある。IT・セキュリティに関して素人である社員であっても、例えば IT パスポートの取得などを通じて、サイバーセキュリティの常識を浸透させていくのも良いのではないか。
- 機械加工・金属加工・食品製造・化学塗料等、OT 環境を持つ中小企業は、運用の停止が事業に直結するため、セキュリティ対策促進の優先度が高いのではないか。これらの企業では、システムの導入よりはむしろシステム運用の失敗が被害に直結する傾向があるため、権限設定やログ復旧を最小限の要件とすべきである。
- セキュリティ人材が不足しているというだけではなく、何を依頼すればよいか中小企業において理解できていないという観点もあるのではないか。セキュリティ人材の確保に当たっては「中小企業向けサイバーセキュリティ対策支援者リスト」を活用するとよいと考えているが、当該リストにおいて、役務・サービスを成果単位でモジュール化するとよいのではないか。
- 昨今、AI をはじめとする技術環境のスピードが高まっており、大企業ですらリスクへの対応が遅れがちとなっているため、中小企業のセキュリティ対策は更に後れをとるのではないかという想定の下で、危機感を高めるべきである。

- 現状トップダウンの視点である経営者側の理解が進んでいないため、各経営者の意識が高い今こそセキュリティ対策の必要性を感じてもらうべきではないか。サイバーセキュリティは投資であるという必要性を理解してもらうためにも、経営層への働きかけを進めてほしい。
- セキュリティ対策を始める前提として、そもそも会社の IT 担当を設置するところから始める必要があるという意見を聞いたことがある。安全責任者や防火管理者の設置義務のように、IT に関しても責任者を設置することで、当該責任者が必要に迫られて IT に関する知見を深めていき、自然とレベルが向上するのではないかという視点である。

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