産業サイバーセキュリティ研究会 WG1
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に関する
サブワーキンググループ(第1回会合)
議事要旨

1. 日時・場所

日時:令和6年7月12日(金) 10時00分～12時00分

場所:オンライン開催

2. 出席者

委員　　:渡辺委員(座長)、江崎委員、教学委員、下村委員、高橋委員、武井委員、古田委員、丸山委員、三井委員、森委員、和田委員

オブザーバ:内閣府、警察庁、金融庁、デジタル庁、総務省、外務省、厚生労働省、農林水産省、国土交通省、防衛省、防衛装備庁、独立行政法人情報処理推進機構

事務局　　:経済産業省、内閣官房内閣サイバーセキュリティセンター

3. 配付資料

資料1 議事次第・配布資料一覧

資料2 委員名簿

資料3 本サブワーキンググループの運営について(案)

資料4 サプライチェーン強化に向けたセキュリティ・アーキテクチャの検討

資料5 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の構築について

資料6 今後の論点(案)

4. 議事内容

冒頭、事務局より、本検討会の趣旨についての説明があった後、経済産業省商務情報政策局 武尾サイバーセキュリティ課長及び内閣官房内閣サイバーセキュリティセンター 山田企画官より挨拶があった。次に、事務局より資料 5、6 の説明があり、続けて自由討議が行われたところ、概要は以下のとおり。

＜制度全体について＞

- オーバーヘッドを小さくする必要がある。本制度のラベリングの対象は企業・組織であると理解したが、別途 IoT 製品に係る制度の検討も進められているため、混同されないように注意されたい。
- セキュリティ対策は導入して終わりではなく運用面も考慮する必要がある。設定の確認やパッチの適用等、運用面でのセキュリティ対策も補記されるとよい。
- サプライチェーン企業が対象となる場合に、一般的に自動車産業のような製造業のサプライチェーンが想起されるが、海外では製造業というよりもソフトウェアも含め、IT サプライチェーンを意味する場合が多く、結果として自分は関係ないということにもなりかねないため、ここで扱うサプライチェーンの定義を明確にされたい。
- 本制度は政府が行う評価制度であり、強いメッセージの発出と強力なブランド化を訴えかけていただきたい。セキュリティアクション(一つ星や二つ星)はある程度普及しているが、その延長として本制度を訴求するのか、あるいはサプライチェーンの範疇で別のものとして訴求するかによって、印象が異なる。前者とすると★1～★5 の認証制度となり複雑となることが予想される。ブランド化の対象については整理が必要である。

・ 全ての基準(★3～★5)を一度に策定することは大変であると考えられる。策定順序に工夫をされたい。
・ ★のレベルが上がるごとに業界固有の要件が増えるため考慮することが難しい。実際に調達や設計、工事で委託する内容が異なる。また、金融や社会基盤インフラのシステムを作る部署や人の契約等、それぞれのサプライチェーンがある中で★3 や★4 の整合性を保つのが難しくなる可能性がある。
・ 調達元が委託先へ★5 を要求する場合に、その先の再委託先等に対しても★5 を求めるのか、あるいは★3 に下げてもよいのかなどをどう判断するのかについても今後検討されたい。
・ 情報漏えいのリスクと業務継続に係るリスクでは、講じるべきセキュリティ対策が異なる。例えば、研究機関であれば重要な技術情報の情報漏えいに対するセキュリティ対策を優先的に講じるべきであるし、銀行であれば業務継続に係るセキュリティ対策を優先的に講じるべきである。このような場合に同じ星としてラベリングするのか。仮に情報漏えいに係るセキュリティ対策が重要でない企業であっても、星を取得するために係るセキュリティ対策を講じなければならなくなる状況にもなり得るので注意が必要である。

＜各業界の対策状況等について＞
・ 製造業では、SEQCD(Safety（安全）、Environment（環境）、Quality（品質）、Cost（原価）、Delivery（工期））という概念が一般的である。「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」は、工場の現場の人達にも認識していただくために、このような用語が用いられているので参考とされたい。
・ サプライチェーン管理の面で、台湾や米国における半導体産業の事例は参考となり得る。
・ 半導体産業に関して、ナショナルセキュリティの観点で、米国や台湾では対策が進められている。米国では退役軍人を雇用して対策を強化している一方で、日本ではそのようなインフラが存在しないと認識している。半導体工場では最先端の技術を使っているため、攻撃を受けて工場が停止すると、製品が台無しとなる。そのような意味でセキュリティ対策は非常に重要である。本検討会では既に進んでいる自動車、金融といた分野の事例を踏み込んでご紹介いただけると非常にありがたい。
・ 例えば、航空事業者がお客様に安全で快適な空の旅を提供するためには、いろいろなサプライチェーンが整備されている必要があるという実態があり、燃料や機内食の食品など様々なインフラが必要となる。

＜制度の対象について＞
・ 評価基準について、資料 5 では「中小企業」という用語を用いているが、中小企業であるから対策レベルが低くてよいわけではない。「自工会/部工会・サイバーセキュリティガイドライン」でのレベル 1～3 でも企業規模による分類は行っておらず、サプライチェーンの重要性や業界の立場等によって求められる対策は何かという観点で分類を実施している。求められる対策についての★3 や★4 等のレベル分けとの認識を有している。
・ 資料 6 の④にも関連する内容であるが、中小企業の規模は中堅企業から零細企業まで実態が様々であるところ、中小企業で一括りしてしまうとミスリードにつながるのではないか。自社に導入されたセキュリティ機能について、中小企業が把握していないケースがある。中小企業が責任をもって★3 や 4 を運用していく形式をとる必要がある。導入ベンダにおいても各段階の対策を運用する仕組みや一定の責任がなければならないのではないか。
・ 殆どの会社においてセキュリティ担当者は 1 人か 1 人にも満たない場合が多い。またガイドラインを作ったとしても、セキュリティ担当者が理解できるように丁寧に説明していく必要があり、そうでないと実際には使われず、有効に働かないケースが多いと感じている。

＜国内外の既存認証制度・ガイドラインとの連携について＞
・ 国内外の制度・ガイドラインの整合性について、米国では NIST SP 800 を参照している。自工会のように各業界でのガイドラインを策定してもらうことを推進するという前提に立てば、まずは基準となるガイドラインを策定することが肝要

ではないか。サプライチェーンの下流に位置する企業はいろいろな業界からの要求事項がバラバラに来ることが予想され、その結果監査等のチェックも煩雑となるので、このようなガイドラインを策定する際に上位のガイドラインとの整合性を取るようにすべきである。

- 交通事業者では国交省のガイドラインを参照してセキュリティ対策が進めてられているが、今回の制度が正式運用された場合、★3～★5 の対策はどこまで求められるのか。各段階で求める水準と既存制度との関係が明確になると事業者側も対策を進めやすいため、関係性の整理をお願いしたい。
- 以前、英国を訪問した際、Cyber Essentials が浸透している印象を持った。国家サイバーセキュリティセンター(NCSC)が制度の普及を強く推進している。また、政府がワークショップの開催を含めたブランド化を積極的に推進している。
- 「自工会/部工会・サイバーセキュリティガイドライン」に加え、金融庁からもガイドラインが公表されており、項目数も多い。対策の必要十分性が重要だと考えており、特に「サプライチェーンにおいて重要な機能・役割等を担う」企業が対象となる★4 の項目数は 50 項目を前提とすることなく検討したほうがよい。金融分野においては金融庁からガイドラインが公表されているだけでなく、米国等でも各種フレームワーク等も公表されているため、参考にされたい。
- ISMS 認証を取得している企業数は 7,800 社以上である。多くの中小企業も取得しており、★4の取得に必要なレベルに達しているのか、疑問が残るところがある。これについては実態をよく調べておく必要があり、ISMS 認証の取得企業が自動的に★4 レベルにあるということには必ずしもならない可能性がある。
- 最初は仕方がない部分もあるのかもしれないが、将来的には他の産業の認証制度等と統合していくのか否かも含めて検討する必要がある。
- 「自工会/部工会・サイバーセキュリティガイドライン」との整合性についてはよく検討いただければと思う。
- 国内外制度との整合性について、業界によってはグローバルにビジネスをしていることから、一歩踏み込んで相互認証まで検討いただけるとありがたい。例えば、イメージとしては、国内で★3 を取得すれば、米国でも★3 の扱いとなるなど。国内にはセキュリティ担当が配置されているが、国外拠点には IT 担当も配置されていないこともあり(例えば、国内では大企業であるが、海外だと中小企業の扱いになる)、認証取得には時間と労力がかかることから、日本のメンバーが支援できるよう相互認証を進めていただければと考える。
- 既存の ISMS、また海外のいまあるガイドライン等との整合性の確認、またそれをどのように担保するのか、さらにリスクに対して同じ会社であっても部門や組織によってミッションが異なるためそれをどう評価するのか、対処項目の粒度もどこまで織り込めるのかについても運用や実装部分において考える上で必要な論点と考えている。

＜基準について＞

- 例えば、自動車と半導体でも産業ごとにインシデントのレベル、社会(内外)へのインパクトが異なることから、業界ごとに異なる固有の要件等も念頭に置きながら高いレベルでの基準の検討を進めるべきである。そのような意味で、半導体分野と同様にバイオ分野やニューロサイエンス分野などもサイバーセキュリティ対策が進んでいる分野と認識しており、これらの分野も内外へのインパクトを整理しつつ検討していくことが肝要である。
- 取扱うサプライチェーンが製造業中心の文脈にも見える、サプライチェーンには業務委託やサービスの利用等も含まれる。モノの供給が止まるという観点に加え、情報(会社のみならず、顧客や従業員のものも含む)が洩れるという観点もあり、こういう要素も論点の中に含めていただきたいと考えている。部品の供給と情報の漏えいという点では対策が異なることも想定されるが、実際に情報漏えいよる影響も大きい点に留意されたい。
- 実際にサプライヤー(サードバーティ)を確認する際、★の数だけでなく、その★を付けた根拠が示される仕組みがあるとよい。
- 星の取得単位について確認したい。例えばある企業が認証を取得する場合、本社で★4 を取得し、ある工場では★5 を取得、ある業務では★3 を取得するという状況になることも考えられるのか。もし、法人単位で取得する場合、★4

を狙おうとすると、不必要な部署まで★4の対策をする必要が生じ、過剰投資が発生する可能性もある。認証を取得する単位をどのようにするか検討する必要がある。

- 評価の星に応じた更新頻度を決める必要がある。また、星を評価する際に、ある時点のセキュリティ対策状況を評価するのか、ある期間のセキュリティ対策状況を評価するのかなどについても制度構築の際に検討する必要がある。
- ISMS 適合性評価制度では細かく言及されていないが、パスワード認証だけとするか、二要素認証まで求めるかなどセキュリティ対策の強度について対策項目に織り込むべきである。

＜認証スキームについて＞

- 自己適合宣言を認める方向性はよい。第三者認証においては認証機関を認定する必要があり、そのための認定機関を設ける必要があるが、認証機関は 1 つとするのではなく、分散させるべきである。
- 評価制度を一元化しない方がよいという意見があったが、実運用する際、評価制度機関について他省庁の制度との関係性や連携等を整理されるのがよい。

＜インセンティブについて＞

- サイバー保険の普及を行う中で、企業のセキュリティ対策状況をどのように評価するかは非常に興味深い。また、日本全体にセキュリティ対策を張り巡らせることを考えた際にサイバー保険はその手段として位置付けられることから、本制度の話を伺った際に大変ポジティブな印象を受けた。
- 導入促進という観点でサイバー保険に係る記載があるが、サイバー保険を購入したい顧客はそれほど多くなく、サイバー保険の割引がモチベーションとなるケースはそれほど大きくないためインセンティブとして機能しにくいのではないか。有事対応の支援や復旧の支援で保険会社を使うことが多く、認証制度の中に組み込んでいただく方が理解しやすい可能性がある。
- 「今後、整理すべき論点（案）」が官主導の書き方になっている点について、制度疲労を起こさないよう、官は調達におけるドライビングフォースとなるなど PR 等で貢献していただき、実態は民間主導で推進するということをポリシーとして持つべきではないかと考えている。そのような観点で、補助金支給ではなく、税制優遇やルールメイキングの施策が重要と認識している。
- 普及面が最も重要である。中小企業ではセキュリティ対策を推進したいが資金が足りないというケースが多いと考えられる。補助金や税制優遇は国としてのセキュリティレベルを高めるために必要かと思われる。また、政府調達を行う上で本制度を活用することも重要なポイントであり、普及の鍵になると考えられる。
- どのくらいの強制力があるのか、またインセンティブは強調していくべきである。
- 中小企業の実態をみて、サイバー保険はセキュリティ対策のひとつになり得ると認識している。事業継続が重要であるという制度にするのであれば、サイバーセキュリティ対策ではないが、事業継続対策として「適切な資金の確保」は検討してもよいのではないか。

＜その他＞

- 取引条件にセキュリティ対策の実装を盛りこむと、公正取引委員会より指導を受ける可能性がある。民主導という意味では、公正取引委員会が所掌する競争法との関係をよく整理していただけるとありがたい。

以上