経済産業省

資料３

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これまでの議論の整理

２０２４年１２月２４日

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

事務局

これまで本SWGでいただいた御意見（抜粋）

【制度の定義】

- 本制度で取り扱う**サプライチェーンの定義を明確**にすべき。

【基準の考え方】

- **既存のISMSや海外ガイドラインとの整合性**や**対策項目の粒度をどの程度まで織り込むか**は、運用や実装部分を考える上でも必要。
- サプライチェーンのリスクには、**製品の供給停止だけでなく**、**情報漏えいの影響等も大きい**ため、制度検討にあたっては勘案すべき。
- **認証取得の対象単位も検討**するべき（例：企業単位や部署単位）。

【対象事業者のイメージ】

- **政府と発注者、評価主体の関係性を明確に定義**した方がよい。
- **発注者が受注者の委託先まで把握できない現状**がある。サプライチェーン全体をみたときにどう捉えるのか。

【他制度・ガイドラインとの連携】

- IoT製品セキュリティ適合性評価制度やサイバーインフラ事業者に求められる役割等、様々な制度が検討されている中、**混同されないように整理が必要**。
- **既存のガイドラインとのマッピング**をお願いしたい。**本評価制度の認証と他の認証との関係性が理解できなければ、事業者の負担が増える**だけ。特に、（同様に段階ごとの対策を求めている）**自工会ガイドラインとの関係性を整理**されたい。

【インセンティブ】

- **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考えられるため、政策的な支援が必要**。
- **最終的には民間主導で制度活用が進められる**よう、ルールメイキングや税制優遇等の施策が重要。
- 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。
- **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。

【その他】

- **取引条件に本制度を盛りこむと、公正取引委員会より指導を受ける可能性**がある。**公正取引委員会が所掌する競争法との関係をよく整理**してもらう必要。

サプライチェーン対策評価制度に関する現状整理（案）①

- 本年3月に制度構想を示して以降、これまで本SWGを2回開催。また、IPAがSC3の下に「サプライチェーンサイバーセキュリティ成熟度モデル検討SWG」を立ち上げ、これまで4回検討会を開催。これまでの議論を通じて、以下の通り制度の概要を整理（個別論点については、年度末を目途とする中間取りまとめに向けて引き続き検討）。

【現状認識（制度検討の背景）】

- 近年、**サプライチェーンを通じた情報漏えい・事業継続に関するインシデントが頻発**。その対策として、政府や重要インフラ企業のみならずその取引先に対しても適切なセキュリティ対策を課す必要があるが、**複雑なサプライチェーン下で、様々な取引先から様々な要求事項を求められている**状況。**発注企業にとっては、正しいセキュリティ対策が取引先でなされているか不明確／受注企業にとっては（特に中小企業を中心に）過度な負担につながっている**。結果として、サプライチェーン全体のセキュリティ底上げにつながっていない。

【制度趣旨】

- **ビジネスサプライチェーン・ITサービスサプライチェーン**における、**取引先へのサイバー攻撃を起因とした情報セキュリティリスク／製品・サービスの提供途絶や取引ネットワークを通じた不正侵入等のリスクに対するセキュリティ対策の成熟度を確認する**（※1）。
- **2社間の契約における発注企業が、受注側に適切な段階（★）を提示し取得を促す**（**再委託先は発注者から見た対象にはならない**（※2））。

（※1）本制度で対象としているのは、あくまで企業体の中におけるセキュリティ対策であり、組織のガバナンス・取引先管理、自社IT基盤への検知・防御等、組織全体に影響が及ぶ範囲を対象としており、ソフトウェア開発やIoT機器のセキュリティを対象にした評価制度・取組とは目的が異なるため、**求められる対策内容や効果も基本的に異なる**。

（※2） **再委託先のセキュリティ対策は、委託先を通じて必要に応じて管理**することも想定（一部基準項目において、「重要な取引先におけるセキュリティ対策状況の把握」を求めることを想定）

【目指す効果】

- **サプライチェーンにおけるリスクを対象**にした上で（※）、その中での立ち位置に応じて必要な対策を提示することで、**企業の対策決定を容易・適切なものにする**。すべてのサプライチェーン企業が対象となるが、特に**サプライチェーンを構成する中小企業は、セキュリティ対策におけるリソースが限られていること／自社のリスクを踏まえてセキュリティ対策を行うことはハードルが高いことから、活用による効果が大きい**と想定。

（※）**本来は各企業が自社のリスクを特定して必要なセキュリティ対策を個別に検討・実施することが望ましい**が、リソースに限りのある**中小企業を中心にただちにこれを実現できていない企業が一定数存在**する。本制度は、**包括的なリスク分析に基づき共通して求められる対策を示す**もの。将来的には、こうした企業も**より自社のリスク分析に基づいたさらなる対策の強化をしていくことが望ましい**。

サプライチェーン対策評価制度に関する現状整理（案）②

【基準の考え方】

- 求められるセキュリティ対策について、**各企業のサプライチェーンにおける重要性や影響度を踏まえた上で、複数区分（★3～5）に分ける**ことを想定。具体的には、**①ビジネス観点（データ保護・事業継続における重要度）②システム観点（接続の有無）の二点で整理**。
- これらの考え方や、**海外での類似制度（英Cyber Essentials）や他産業のガイドライン（自工会・部工会ガイドライン、他分野別ガイドライン等）の記載**を踏まえつつ、NISTの「サイバーセキュリティフレームワーク2.0」等にも基づき、「ガバナンス整備、取引先管理、リスクの特定、システムの防御、攻撃等の検知、インシデントの対応・復旧」の観点から、**★3・4の考え方、対策事項・要求項目について整理**を行った。
- **★3は基礎的なシステム防御策と体制整備を中心に構成**。**★4はガバナンスから防御・検知・対応まで包括的な対策**とすることを想定。

（※） ★5については、より高いレベルの対策としては、前述の通り自社やサプライチェーンに対するリスクアセスメントの考え方が求められるため、**各企業におけるリスクに応じて対策を講じることを求めるISMS適合性評価制度との制度的整合性も含めて、位置づけ・基準を検討。**

【国内外の関連制度等との連携・整合】

- 先行する自己評価の仕組みである**「SECURITY ACTION」「自工会・部工会ガイドライン」**や前述した国際標準である**「ISMS適合性評価制度」**とは、**相互補完的な制度として発展することを目指す**。
- 具体的には、**現在の★3・4の要求項目案は自工会・部工会ガイドラインとも対応**しており、自工会・部工会ガイドラインに基づく自己評価に際しての本制度での活用等、**連携のあり方については、運営団体とも議論を進めていく**。また、**海外の類似制度**についても、**将来的な相互認証の可能性も念頭に、引き続き調査・意見交換を実施**する。

サプライチェーン対策評価制度に関する現状整理（案）③

【制度において設ける段階の考え方】

	★3	★4	★5（※）
想定される脅威	• 広く認知された脆弱性等を悪用する**一般的なサイバー攻撃**	• **供給停止**等によりサプライチェーンに**大きな影響**をもたらす企業への攻撃 • 機密情報等、**情報漏えい**により**大きな影響**をもたらす資産への攻撃	• **未知の攻撃**も含めた、**高度なサイバー攻撃**
対策の基本的な考え方	• 全てのサプライチェーン企業が**最低限実装すべきセキュリティ対策**として、**基礎的な組織的対策とシステム防御策**を中心に実施	• サプライチェーン企業等が**標準的に目指すべきセキュリティ対策**として、組織ガバナンス・取引先管理、システム防御・検知、インシデント対応等**包括的な対策**を実施	• **高度なサイバー攻撃にも対応可能なセキュリティ対策**として、**リスクベースのアプローチ**に基づく改善プロセスを整備した上で、**リスクに応じて必要な対策**を実施
脅威に対する達成水準（イメージ）	• **組織内の役割と責任が定義**されている。 • 一般的なサイバー脅威への対処を念頭に、自社**IT基盤**への初期侵入、侵害拡大等への対策が講じられている。 • インシデント発生時に、**取引先を含む社内外関係各所への報告・共有に必要な最低限の手順が定義、実施**されている。	• セキュリティ対策が**組織的な仕組みに基づいて実施され、継続的に改善**している。 • **取引先のシステムやデータを含む内外**への被害拡大や攻撃者による目的遂行のリスクを低減する対策が講じられている。 • **事業継続に向けた取組や取引先の対策状況の把握**など、自社の位置づけに適合した**サプライチェーン強靭化策が講じられている**。	• **リスクアセスメントの結果**を踏まえ、**システムへの具体的な対策の実装や状況把握に基づく改善プロセスの運用**がなされている。 • 組織における**マネジメントシステムが確立**されている。
評価スキーム	**自己評価** （※）記入内容については、専門家が問題ないか評価を実施	**第三者評価**	**第三者評価（★4と同等）**
ベンチマーク （対象企業やリスクが同様であり、対策項目を検討する上で参考）	• 自工会・部工会ガイドLv1 • Cyber Essentials ⇒★3で対処する脅威等に照らして精査し、対策事項（案）を抽出	• 自工会・部工会ガイドLv2～3 • 分野別ガイドライン 等 ⇒★4で対処する脅威等に照らして精査し、対策事項（案）を抽出	• ISO/IEC27001 等 （※）各企業におけるリスクに応じて対策を講じることを求める**ISMS適合性評価制度との制度的整合性も含めて、位置づけ・基準を検討**

本制度の推進にあたって必要な検討事項

事項	論点	検討の方向性
①企業に対する働きかけ①（発注企業のためのルール整備）	• 制度を活用すること（取引先に対する対策の要請）が、下請法等の既存のルールに抵触しないか、わかりやすく示す必要。	• これまで、経産省・公正取引委員会によるガイドライン（「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」）等が示されているが、これらの既存の取組も踏まえた上で検討を進める必要。
②企業に対する働きかけ②（取得企業に対する支援）	• 中小企業に対しては、これまで「サイバーセキュリティお助け隊」を通じて安価で利用可能なサービスが提供されてきたが、お助け隊でカバーされない対策が求められるのか。 • お助け隊のみならず、中小企業が対応するにあたって、専門人材等の人的リソースが不足している懸念点も考えられるが、どのようなアプローチを行うのか。	• 中小企業からは、下記のような懸念を持つことを想定。 ①対策項目を踏まえてどのような対応を行えばよいかわからない ②金銭的／人員的リソースが不足している • これらについて、「サイバーセキュリティお助け隊」や登録セキスペの拡張・活用等も含め、必要な対策を講じる。
③企業に対する働きかけ③（制度普及にあたっての初期ターゲットの設定）	• 今後、本制度の普及を進めていく中で、どのような業界で優先的に進めていくべきか。どのような考え方で決めるべきか。 • また、当該業界において普及を進める際、どのような施策を講じることが効果的か。	• 政府機関や重要インフラ分野、主要製造業が想定されるが、詳細についてはSC3下での検討会でも議論の上、今後本SWGでも提示予定。
④制度の導入促進にあたっての環境整備	• 企業が本制度を取得する上で、評価機関や検証事業者、助言専門家（例：登録セキスペ）等の環境整備が必要になるが、その確保のためにどのような取組を行うべきか。	• SC3下での検討会でも議論の上、今後本SWGでも提示予定。
⑤制度の運用体制	• 評価スキームをどのように構築すべきか。また、制度を運営していくにあたり、運営主体や認定機関はどういった者が望ましいか。	• 評価スキームについてはSC3下の検討会で議論を行い、海外制度も踏まえ、★3を自己評価／★4は第三者評価とする形で検討中。 • その上で、制度運営者に必要な機能・体制をSC3下の検討会でも議論した後、本SWGでも提示予定。