# 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3回会合)
# 議事要旨

## 1. 日時・場所

日時:令和6年12月24日(火) 10時00分～12時00分

場所:オンライン会議

## 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 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(案)

参考資料1 SC3業界連携WG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における事務局資料【委員限り】

## 4. 議事内容

事務局より資料 3 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＞

- 制度とガイドは異なるものであり、制度を構築することが前提となっている点に違和感がある。企業等が取り組むべき事項のガイドとそれを評価するための制度をバンドルし過ぎているのではないか。
- 本評価制度は ISMS 制度に足りない部分を拡充する制度、ISMS を取得するための組織の整備に資する制度という位置づけが、理屈的にすっきりするのではないか。
- 昨年、英国 CE について業界団体へのヒアリングを行ったが英国政府の制度という印象が強かった。国にお墨付きをもらうことで、企業における取引上のステータスとなっているようである。日本においても、政府が前に出てメッセージを出すべきものと理解している。業界に任せるより、国として制度化を目指すべきと考える。
- 制度化については煩雑になることも承知しているが、グローバル市場を気にする企業であれば財務諸表等で対策状況を気にするようになっている。制度の是非は難しいところではあるが本制度はあった方がよい。海外制度とのハーモナイゼーションも含めて、日本の産業界にとってはメリットになるのではないか。
- 自動車業界では、各社が保有する在庫を少なくした上で製造を行っているため、サプライチェーンの断絶が大きな影響を及ぼす。本制度も、サプライチェーンの全体のため取組として理解すべきである。業界全体で取り組むことが望ましい。

＜制度趣旨について＞

- 通信業界では大きな会社が発注者になるが、グループ会社や中小含めて様々な企業が存在している。指標だけでなく運用を含めて受注側の負担を減らす仕組みとする点が重要である。発注者が★を求めるのは簡単である一方で、対応する受注者は手間がかかる。社会全体で★を取ることによる効果が共有されることが普及にとって重要となるのではないか。
- 英国 CE は 2014 年から開始してから、3 万 2 千社もの 250 名以下の企業が取得しており、マネジメントシステムというより具体的な対策に重点をおいている基準である。また、売上が 2000 万ポンド以下の企業に対して、インシデント時の無料の駆け付けサービスを含むサイバー保険が提供されている。CEは政府の取組であるため、その費用負担は国民全体が行っていることになり、非常に参考になる点である。NCSC が中心となり運用されている CE を中小企業が取得することで、箔が付く仕組みとなっている。日本においても、費用負担やサイバー保険の付帯等を恒常的な仕組みに取り入れるとともに、中小企業に対しても取得しやすい環境を整備することで、本制度によって社会全体がよくなるという点をブランディングしては如何か。
- セキュリティ被害がサプライチェーンの他社にも及ぶため、個々の企業の利益判断だけでセキュリティ対策を検討されても全体が困る側面がある。本制度は公益の目的がある点を明確にされたい。一企業の判断の側面もあるが、公益のために必要という説明とすべきである。中小企業に対して支援を行いつつ、多くの企業に本制度に参加いただくことがよい。
- 受注側からみても、コストや使い勝手という面で本制度にはメリットがある。本制度は、個々の企業だけでなく社会全体のレベルアップにつながるものであり、公的な支援につながるとよい。
- 本制度は、最低ラインを定めるものと理解した。サプライチェーン全体の底上げを図るものである一方で、本制度は発注者と受注者間の関係性を軽く捉え過ぎてしまうと、各種業界のガイドライン等に充足し切れないものになってしまい、結果として温度感の異なるものになってしまう可能性が高いため、メッセージの出し方は考慮されたい。
- 本制度は国がメッセージを出しサプライチェーン構成企業にセキュリティ対策働きかけるものと理解した。保険業界ではサプライチェーンを構成していない企業にもセキュリティ対策を働きかけているが、サプライチェーンを構成していない企業は本制度の対象外か。

  ⇒（事務局）基本的にサプライチェーンリスクにフォーカスしている。サプライチェーンを構成していない企業に対してはサイバーセキュリティお助け隊サービスを含めた中小企業向けの施策をパッケージとして提示したい。ただし、評価を受けたい企業を排除する必要はないと考えている。

＜第三者認証について＞

- 資料 3「サプライチェーン対策評価制度に関する現状整理（案）③」(P.5)に示された第三者評価を企業はなぜ利用しなければならないのか。内部統治の一環で該当組織が判断する事項ではないか。本制度を利用しなくてもしっかりと対応がなされていれば、商取引として問題ないという建付けがよいのではないか。例えば、IPA は自動車と蓄電池のトラストデータを登録するシステムを構築し、Catena-X と連携させようとしているところ、当該プラットフォームの利用判断は事業者に委ねられている。本制度についても同様ではないか。
- 第三者認証を採用する場合に、企業側でかかる費用が問題となる。第三者認証時の評価を精緻に行えば、より多くの費用がかかる。企業側でかかる費用感の目標を立てつつ、検討を進めるべきと考えている。他方で、それぞれの取引先や業種や業態に応じて費用の多寡は変わり得るという指摘があり、その目標とは切り離して考える必要がある。
- 現在は、発注者が定めた基準に基づき、発注者は受注者に対してセキュリティ対策状況を個別にヒアリングしている。各社が定めた基準による対応が発注者と受注者双方の負担になっているため、本制度の検討が開始されたと認識している。
- 特に★4 の場合、受注者における評価の正確性の担保を発注者は求めるが、自己評価だけでは発注者は十分と捉

えない場合があるのではないか。受注者としてはコストとなるが、第三者評価は発注者にとって頼りになる。

- 第三者認証や監査にはコストがかかる。保証の水準にはレベルがある。精緻に確認を行う会計監査には非常にコストがかかる。他方で、ISMS 適合性評価制度における監査は会計監査と比較すると、確認の精緻さの面で緩い。コストと確認の程度はトレードオフの関係があり、社会的にどこまでの確認を求めるかは議論を行った上でコンセンサスを得る必要がある。
- 保証業務で見落としがあると訴訟になり得る。コストとメリット、認証機関のリスクを含めて定量的な分析も必要となる。
- 公開情報によると英国 CE において、年間 3 万 4 千社が申請を行い、1万1千社が CE+の認証を取得している。CE+を取得している企業のうち、250 名以上の規模の企業は全体の 16%であった（申請を行っている企業全体の中の 10%)。CE のように認証の取得要否を事業者の判断に任せることができないか。例えば、認証を受ける場合はゴールドとして追加で評価し、金銭的に余裕のある企業が認証を受ける形とする。認証を受けていることで CE と CE+のように別の表記を得られるようにしてはどうか。認証の有無で★4 を分けることも一案である。

＜制度運用について＞

- 本制度を普及させるためには、★3 や★4 の取得基準（達成基準）を明らかにすることが必要である。また、発注者の立場からすると、取得した★の提示(特に★4 の場合)だけでは十分でないケースも想定される。発注者が、評価項目に対する評価結果の状況のレポーティングを受注者に求めることも考えられ、そのような取組もできる枠組みとなっているべきである。そのような取組が認められるものでなければ、発注者からすると使いやすい制度とならない可能性がある。
- 取引関係におけるプロトコル(手順)が制度のドキュメントに明示されることは有益であり、制度を円滑に運用するためには重要である。
- 発注者によって委託内容や調達物により受注者に求めるセキュリティレベルは異なる。受注者は企業によって求められる★が異なることで混乱を招き得る。本制度の円滑な運営のためにはそのような混乱をできるだけ小さくする必要がある。
- 企業の中には、グループ経営を行っている企業があるが、グループ会社を含めてすべて同じレベルである必要があるか。ホールディングスに責任を持たせた上で、そのホールディングスの自主性に任せて、そのレベルを決定させることも普及の施策と考える。
- 資料 3「サプライチェーン対策評価制度に関する現状整理（案）③」(P.6)の「⑤制度の運用体制」で評価スキームが論点として挙げられている。ここは時間をかけて検討する必要がある。認証ビジネスができる際にある機関に独占させるのではなく、評価機関・審査機関の能力評価も行い、認定を受けた機関が実施できるとした方が競争も発生する。コスト圧縮効果も働くのではないか。Common Criteria(CC)認証のスキームを参考にされてはどうか。

＜制度の普及について＞

＜全般＞

- 本制度の対応にかかる費用(有償/無償)が気になる。有償の場合、企業にとって認証を受ける際のハードルとなり得る。政府が補助を行い、有償でも制度が普及するよう努められたい。
- 半導体業界の部素材メーカーはグローバルサプライチェーンに含まれている。上流に行くほど 1 つの企業に集中している傾向があり、そのメーカーがサイバー攻撃を受けるとサプライチェーン全体に大きな影響が及ぶ。そこには余力のない中小企業も含まれているため、政府から中小企業に対してセキュリティ対策に係る支援をしていただきたい。
- 自動車業界におけるフィジカルなサプライチェーンには 8 万社～10 万社が含まれているとされているが、自工会ガイドラインを踏まえた自己評価の回答は 4 千社程度にとどまっている。1 企業の取組では限界があるため、政府として様々な施策を検討いただきたい。政府と民間が協力しながら推進していくべきである。

・　サイバーセキュリティは経営課題ということが広く言われている。本制度においても、経営者に直接アプローチすることで普及啓発を行うことが重要である。経営層に刺さる普及施策が重要である。

＜サイバー保険、初動対応について＞

・　資料 3「これまで本 SWG でいただいた御意見（抜粋）」(P.2)について、インセンティブに「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。」とある。前回の SWG では、本制度普及のモチベーションとしてサイバー保険料が安くなる点に焦点が当たっていたが、サイバー保険を運営している側は決してそのようにとらえていない。むしろ、最近は中小企業がインシデントを受けた際に相談可能なインシデント初動対応支援機能にサイバー保険のニーズがあるようである。資金の確保に加え、インシデントから早急にリカバリーするための機能として、本制度でもサイバー保険の役割を定義いただくことが効果的と考える。
・　初動対応支援の観点は重要であり消防署の機能と似ている。国として支援することが必要である。
・　可能な限り、具体的な方法がわかるようにドキュメント整理を進めることが重要である。対策について抽象的な表現ととどまっており、具体的な対策に係る情報が不足している。産業界が各々検討して対策を進めているが、国からも情報を発信すべきである。
・　単なる資金ではなく、実際に行う活動(例:インシデント対処)の支援も国から行うことが必要である。

＜サイバーセキュリティお助け隊サービスについて＞

・　サイバーセキュリティお助け隊サービスの 1 類サービスには価格の上限があり、現状のものは提供側（ベンダー）にとってハードルが高い部分がある。★4 では 2 類サービスになると予想されるが、2 類サービスは 1 類サービスの提供を前提としているため留意が必要である。1 類サービスの提供がなくとも、企業が 2 類サービスを提供できるようになるとよい。なお、サイバーセキュリティお助け隊サービスは IT 導入補助金の要件となっておりインセンティブになっている。

＜他制度との関係について＞

・　取引先等から様々なセキュリティに関するヒアリングを受けている企業のセキュリティ担当はコンプライアンス対応に業務の大半の時間をとられており、本制度もこれらの実態の one of them になると現場の混乱を招く可能性がある。本制度の利用に、その他の発注元からの要求を代替できる等のステータスがあると、企業のセキュリティ担当はコンプライアンス対応から、より有効なセキュリティ対策に多くの時間を割けるようになる効果が出るのではないか。
・　本制度によって、よりスムーズで健全な受発注となることが重要である。電気事業法に則して既存のセキュリティガイドラインがあり、サプライチェーンのセキュリティについても電力サブワーキンググループの検討内容を適用することとなっている。当該 SWG では「電力制御システムにおけるサプライチェーン・セキュリティ向上策に関する提言」がなされており、そのような既存取組や制度と整合を保つことで、企業の負担感を減らすことにつながるのではないかと考える。
・　海外の顧客からセキュリティ認証を求められるケースがこれから増えていく。半導体市場は海外顧客が中心であるので、海外の制度との相互認証をぜひ実現いただきたい。
・　IoT 製品の適合性評価制度と同様に、グローバルとの整合性確保が非常に重要である。
・　制度構築後も本評価制度は随時更新される想定か。 ⇒（事務局）情勢に応じて基準は更新する予定である。
・　中長期的には、本評価制度と自工会ガイドラインを 1 つに統合していくことも想定されるが、更新自体に手間がかかるとともに、双方が残り続けると受注者も混乱し得る。今は相互補完の関係として、中長期的に考えていきたい。

＜資料 3 の記載について＞

- 資料 3「サプライチェーン対策評価制度に関する現状整理（案）①」(P.3)では、「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。」と記載されている。「自社のリスク分析に基づいたさらなる対策」とは、利害を共有するサプライチェーンを構成している企業群が「包括的なリスク分析」によって決めているベースラインを超えるものと理解している。「自社のリスク分析」と「包括的なリスク分析」を別に行えばよいと誤解されないよう記載して欲しい。また、「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。」と記載されているが、サプライチェーンでの包括的なリスク分析があった上で、自社でのプラスアルファの分析があるという構造を示すべきである。
- 資料 3「サプライチェーン対策評価制度に関する現状整理（案）①」(P.3)には、「再委託先は発注者から見た対象にはならない」との記載がある。発注者からすると、受注者の再委託先のセキュリティ対策状況は気になる点である。
- 資料 3「サプライチェーン対策評価制度に関する現状整理（案）①」(P.3)の「制度趣旨」にて、「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」とある。現在の表現では、発注者が取得を促すようにもみえるため、適切な表現を検討頂きたい。

以上