# 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4回会合)
# 議事要旨

## 1. 日時・場所

日時:令和7年2月28日(火) 9時00分～11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、森田様(高橋委員代理)、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 対策の基本的な考え方と要求事項案・評価基準案

資料4 制度普及に向けた考え方・取組

資料5 今後の検討の進め方及びスケジュール

参考資料1 ★3・★4要求事項案・評価基準案一覧

参考資料2 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 中間取りまとめ(素案)【委員限り】

## 4. 議事内容

事務局より資料 3、資料 4 及び資料 5 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。

＜制度の更なる詳細化について＞

- 本制度について、丁寧な整理となっている。参考資料 1 で要求事項・評価基準が示されているが、★4 の取得には★3 の取得が前提となるのかどうかがよく分からない。制度運営上の手間となる可能性があるため、★3 を取得しなくとも、★4 を取得できる枠組にしていただければと思う。
- 全体としてまとまってきた印象である。★3 と★4 の関係性が気になっている。★3 は境界型防御を行い、★4 はネットワーク内部の監視等も行いつつ、多層防御を行うでと理解した。その上で、★4 を取得する際に★3 の維持は前提となるのかについての整理が必要と感じた。
- 日本自動車工業会(以下、「自工会」という。) では、レベルに準拠する際の順番は問題にしていない。★3 から取得できないとする場合、レベルダウンしたところから始まる企業がでてくるため、★4から取得できるように検討されたい。
- 発注者の立場で考えた際に、★3 や★4 の提示だけでは満足できない側面がある。依頼主の希望により、更に詳細な情報を開示いただけるような仕組みを検討されたい。
- 制度の検討が進み、全体としてまとまってきた印象である。資料3の「制度で用いるセキュリティ要求事項・評価基準」

(P.3)について、★取得の有効期限などは議論しているか。★を一度取得した場合、そのままで良いのか。定期的な更新の方法について決めておくべきではないか。★3 では 2 パターン考えられ、ISMS や ISMAP に倣って有効期限を定めることや、あるいは取得年月日を併記する等の対応が考えられる。★4 では定期的な見直しが必要なのではないか。

- 有効期限は慎重に議論すべきである。有効性とコストの関係性を踏まえつつ、来年度の実証の中で答えを出していくべきではないか。
- 本制度のスコープについて、★の取得単位(例:企業単位、プロジェクト単位)を明確化いただきたい。小さな企業では会社全体での取得もあり得る。★の取得単位を明示しなければ、示された側がうまく受け止められないのではないかという指摘である。
- 非常にまとまっており、資料としては大変良くなったと感じているが、大企業、中小企業の双方で、★3 レベルと★4 レベルのシステムが混在している状況ではないか。この場合にはどのような評価がなされるのか。本制度を活用する側としてもコストが下がるように運用したい。サプライチェーン構成企業の対策状況を把握する必要があるが、★3 取得済みであれば、ある程度対策はできているとして、細かな調査は不要となると良い。
- 評価機関や検証機関についての資格要件も考えたほうが良いのではないか。CC 認証のような厳密なルールまで求める必要はないと思うが、評価機関や検証機関の要件をそれぞれ整理すべきである。
- 実証の中で、評価する上での費用や工数を確認、検証するとのことだが、非常に重要であるため、ぜひ実施いただきたい。
- 適用の限界について、まずは適用してみて問題があれば挙げていただくというスタンスで良いのではないか。

＜要求事項・評価基準の詳細化について＞

- 資料 3 の「制度において設ける段階」(P.2)において、★3 や★4 の概要が示されているが、どのような企業が★3 や★4 の対象と想定するのか、具体例を示しながらよりブレイクダウンしたガイドを作成いただけるとありがたい。
- 保険業界としては、保険の引き受け時にセキュリティ対策を確認しており、また委託先(例:代理店)のセキュリティ対策についても確認している。その中で、セキュリティ対策の方法がわからないとのご指摘をいただくこともあり、初歩的かもしれないが、セキュリティ対策の実装方法や支援策等の配慮も必要と考えている。
- セキュリティ対策やその実装方法に係るノウハウがなく、困る事業者やガイドラインをみたものの、わからない事業者や評価基準がわからない事業者が多い。また、横文字の会社に相談できない企業も多く、このような点について業界でも取り組んでいるところ、届く範囲に限りがあるため、政府としても丁寧な対応をお願いしたい。
- ★5 では ISO 27001 が参照されている意図を確認したい。各業種のガイドラインは NIST の文書等を踏まえて作成されており、ISO 27001 だけが参照されている点に違和感があった。
  ⇒(事務局)ISO の参照について、業界ごとのガイドラインと ISO 27001 では粒度が異なるため浮いているように見えるとの指摘と理解した。ISMS を提示した理由は、チェックシート的な対応よりは高度な対策に備えたリスクベースの対応を行うニュアンスを示すためである。
- 実証事業を行うにあたって、評価基準が定まっている必要がある。
- 資料 3 の「制度で用いるセキュリティ要求事項・評価基準」(P.3)について、特に「サプライチェーンの防御」に関連するが、半導体業界では前工程と後工程があり、日本の中で完結できているわけではなく、世界中で分業する体制となっている。ウエハー自体は日本で作るが、後工程はアジアで行うケースが多く、拠点の多くは資本関係のない他社が後工程を行うこともあるため、海外企業にガイドラインを適用できない可能性があり悩ましいところである。

＜制度運営基盤の整備について＞

- 資料 5 の「実証事業の推進計画」(P.3)に関連して、本制度の運営機関すなわち制度オーナーはどこになるのか。言

い換えると、評価を進める中で責任を負う主体、ユーザー企業の苦情対応等を受けるところはどこか。
⇒（事務局）制度オーナーは経産省や IPA が該当するとの認識であるが、実務面も含めて運営や管理を行う機関としてはまだ明確に決まっているものではなく、他の制度状況等も踏まえた調整も必要になる。

- 第三者評価を要する★4 では、評価を受ける際のコストが一定程度発生すると思われる。実証実験を通じて確認することになると思うが、評価を受ける側が評価を受けやすくなるような負担の適正化をお願いしたい。なお、評価を受ける側にとっても、対策の点検をする良い機会となる点は、制度の普及にあたってのアピールポイントとなり得る。
- 一方で、★3 は自己評価であることを踏まえると、評価者自身の評価スキルを高めていく必要がある。「サイバーセキュリティお助け隊サービス」の活用も含め、様々な教育施策等を並行して行うことが重要である。
- 中小企業を対象とした取組も重要だが、評価を受ける対象には大企業や中堅企業も含まれており、大企業や中堅企業を対象としたメッセージも準備されると良い。

＜制度の普及について＞

- 運用普及に向けて、周知はしっかりとした方がよい。日本商工会議所や経済同友会を含めて連携されたい。IPA には良い資料がたくさんあるが、あまり周知されていないケースがある。しっかりとリファーされることが望ましい。
- 本制度に係る情報が公開された際に、国として非常に強いメッセージが出るものと理解しており、国としてのメッセージを気にされている企業が多い印象を持っている。普及の部分で、業界にある程度活用いただくためにどうすれば良いかという書き方となっているが、例えば国としてもう少し強いメッセージがあると発注者側にも伝わり、より制度が周知されるようと思われるが、国が潤滑油としてルールを作り、あとは業界における相対の契約にゆだねるというスタンスで合っているか。
  ⇒（事務局）資料 4 の「制度の導入促進」(P.5)とも関連するが、本制度が効果的に働く業界もあると考えられる。活用の方向性など施策も含めて関係機関と検討したい。
- サプライチェーンの構成企業が本制度の対象でありつつ、自社が対象外と認識している企業もあると考えられる。国としての評価制度はインパクトがあるため、そのような企業もぜひ取得していただけるよう対象やスコープを拡げるような検討も進めていただきたい。
- 金融業界では、委託先の大半が別の業界となっている。本制度の普及に当たっては業界横断的に進める必要がある。
- 自動車業界では在庫を抱えない体制となっているため、発注者や受注者だけでない業界全体として取組を進めている。日本全体のため、という視点で本制度を説明いただきたい。
- 自工会の経験では Tier3 以降には伝わらないことが多いため、プロモーションの面で政府には期待している。
- 実証実験等を通じて、★の取得企業数に係る目標(例えば、1万社とするなど)を設定すべきである。ISMS をすでに取得している事業者では、対応がある程度容易なはずである。政府機関横断的に協力して普及促進を行うべきである。
- 普及を主眼に置いて来年度から事業者を巻き込んで取り組むとよい。
- 投資ではなく必要なコストという議論になってきている。財務的なインセンティブ、例えば税制などをパッケージとして考える段階に入っている。来年度は制度単体ではなく、コストを払えるための総合的なパッケージとして検討を進めるとよい。
- 大企業が発注者の立場で、サプライチェーン構成企業に対して何かを要求する場合、下請法や独占禁止法の面で不当な要求とならないよう注意を払っている。この制度に基づく受注側に対する要求が、下請法や独占禁止法に抵触するような扱いとならないよう、広報や、法令との兼ね合いの調整をしっかり行っていただきたい。
- セキュリティ対策の人材を育成するためにどのような施策があるか。半導体業界では、世界中でセキュリティ人材が不足していると言われている。事務局としてはどのように考えているか。

⇒（事務局）本制度に限らず取組として重要なところ、「サイバーセキュリティ人材の育成促進に向けた検討会」での検討の中で検討を進めているところである。なお、資格取得後に情報処理安全確保支援士資格が活用されていないという指摘もあるため、マッチング促進等の取組に加え、全体のパイを増やすような取組等も検討している。

・ 人材については重要インフラについては IPA の産業サイバーセキュリティセンター(ICSCoE)がリーダーの育成の点でうまくいっている。それ以外の業界でどのように実施するのかを検討されたい。

＜その他＞

・ 資料５の「実証事業の推進計画」(P.3)に示された「調達者」の記載はわかりにくいため、「発注者」等の表現に修正するとよい。

・ 参考資料１に示す要求事項/評価基準について、どのように読めばよいかを明記いただきたい。例えば、★3 の要求事項と★4 の要求事項の遵守にあたって、AND 又は OR なのかで迷う場合が多い。

以上