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6回会合)
議事要旨

1. 日時・場所

日時:令和7年12月23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、中西委員、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、内閣官房国家サイバー統括室

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実証報告書

資料4 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制度構築方針(案)

別添　★3・★4要求事項及び評価基準案

4. 議事内容

事務局より資料の確認があった後、渡辺座長が議事進行をした。

委託先事業者の日立製作所が資料3を説明し、事務局が資料4を説明した。続けて自由討議が行われたところ、概要は以下のとおり。

＜実証報告書について＞

・　近年のセキュリティインシデントを受け、企業間で本制度への対応が不可避との認識が広がっている。実証参画企業の受け止めを伺いたい。

⇒実証参画企業は本制度に前向きな姿勢。一方で、一部の要求事項への対応が難しい企業もあり、セキュリティ水準を維持した上で許容する方策を増やす等の、一部内容の更新を行った。

・　対応が難しい要求事項に代替策を認めると、要求事項と評価基準が合致しなくなるのではないか。

⇒セキュリティ目標を下げることなく、手段の多様化で対応しており、要求事項と評価基準との整合性を担保している。

・　評価基準を全て満たさなければ★を取得できない方針については賛成だが、不適合項目がある場合の評価結果の活用は可能か。

⇒全ての要求事項を満たすことが★取得の大前提となる。★4では、不適合項目があっても、評価者が申請者にフィードバックを行い、一定期間内に改善すれば★取得が可能な仕組みとしている。

・　取引先との間でセキュリティ対策状況を把握し、発注元がリスクを踏まえて契約判断を行うことはルールの範囲内であり、公的機関からの不適合項目の開示も重要である。

⇒全ての要求事項を満たすことで★を取得できるが、一部満たしていない部分について、公的機関からの開示は困難。二者間の取引において提示し考慮することもあり得る。

- セキュリティ水準を下げない方向性と、不適合項目の開示結果を取引で考慮することを認める方向性が共通認識として明確になっていればよい。
- 現時点で全ての要求事項を満たせていない実証参画企業からの要望はあったか。
  ⇒要求事項を満たせていない中小企業、中堅企業を中心に、サイバーセキュリティお助け隊や補助金等による支援を要望する声が存在。
- 実施工数が多くかかっている企業があるが、ばらつきの差は企業規模によるものか、業務内容によるものか。
  ⇒事業規模の相違が一因。適用範囲をグループ全体とした場合、多数の関係者が関与することから、必要となる工数が増大したものと認められる。特に、大企業においては、関係者の数が多いことから、個々の対応時間が短くとも、全体としての実施工数が著しく増加したものと推察される。
- 第三者評価にどの程度の工数がかかったか。
  ⇒資料3に示された工数は実績値。示した工数の範囲で対応いただくよう評価機関に依頼をしている。
- 取引先に対して同じような取組を行っている発注元企業が本制度との統合について言及していたが、詳細を知りたい。
  ⇒当該企業は、ISMS や NIST SP800 を参照しつつ、親会社のセキュリティ部門が独自の基準を策定し、これをグループ会社に適用する枠組みを運用。公的な制度として本制度の利用可能であれば、当該制度を参照先とすることが望ましいとの意向であり、状況に応じて本制度への統合も検討する考えである。
- ★3の取得に際しては専門家による評価が要件とされているが、多くの企業においては社内に専門家が在籍していない事例が散見。実証事業においては、内部専門家と外部専門家との間で評価に差異はあったか。また、サイバーBCP の要素が導入されたことについて、各企業が必要と認識した事項についても確認したい。
  ⇒実証には、現地での打合せや証跡確認、コンサルティング等を実施した専門家がいる一方、書面によるアセスメントシートの確認のみ対応した専門家も存在。対応内容及び所要工数に専門家間で差異が認められた。制度の本運用においては、セキュリティ専門家に対し研修の受講を予定しており、専門家間の対応のばらつきを抑制する方針。サイバーBCP については、業界団体や実証参画団体から、完璧なサイバーBCP を求めることは困難だが、まずは検討を開始することが重要であり、継続的な改善を図るべきとの意見が示されたことから、サイバーBCP の要素を要求事項に含めることとした。

＜構築方針案について＞

- 要求事項と評価基準の整合性の確保が求められる。加えて、各企業が自社の評価結果にアクセスできるようにする必要がある。不適合項目については明確化することが望ましい。また、本制度の対象が IT に限定され OT は対象外であることを明示すべき。
  ⇒1点目については、ご指摘のとおりであり、企業が自社の評価結果にアクセス可能な仕組みとする方針である。2点目については、ご指摘を踏まえ、制度の対象範囲の明示方法等、見せ方について今後検討を進める予定である。
- 評価機関の指定は、資料に有効期間の記載がないため、有効期間（例：2年間）を設定し、継続的なサーベイランスを行うべき。また、評価機関の要件については、現状よりも要求水準を引き上げる余地があると感じた。今後、CC（Common Criteria）認証を参考にしつつ、要件の粒度をより細かくしていただきたい。
  ⇒資料に記載した第三者評価機関の要件は、運用開始に向けて今後詳細化を進め、別途文書として整備する予定である。また、第三者評価機関の指定に係る有効期間については現時点で詳細は未定であるが、有効期間を設けることを想定しており、今後具体的に検討を進める方針である。
- 一方で、評価機関に対する要件を厳格化することにより、評価サービスの価格が上昇する可能性があるため、評価

機関の候補と調整を行いながら、要件の具体化を進めることが望ましい。

⇒本制度は中小企業による活用を目指しているため、評価機関の要件設定にあたってはコストとのバランスを踏まえて検討したい。サービス価格の上昇は普及の阻害要因となり得るため、バランスのよい制度設計に努める。

- 大企業もセキュリティインシデントからの復旧に時間を要している。中堅中小企業がインシデント対応を行う場合、対応すべきことが多岐にわたるため、BCP があったとしても機能しないことがある。制度側がインシデント対応時に実施すべき項目を明確にした上で、中堅中小企業はその項目を事前に理解しておくことが重要。別添資料にて示されている要求事項及び評価基準には、平時の対応が含まれている一方で、有事の対応が詳細に定義されていない。保険業界も細部で力添えできるとよいと考えている。

  ⇒サイバーBCP の対応については、具体化が必要であると認識しており、要求事項を補足するためのガイダンス等の資料について、ご指摘いただいた事項を踏まえつつ、充実を図ることが重要である。
- 資料4に関し、独占禁止法及び取適法（旧下請法）上「問題とならない」とされる想定事例が示されているが、発注元からセキュリティ対策の実施を要請された企業が、★3★4の対策事項を未実施である場合、ゼロベースでの対応が必要となる可能性がある。その場合、要請への対応コストが製品価格に転嫁され、発注元にも影響が及ぶ。

  ⇒セキュリティ対策コストは、サプライチェーン全体での負担も想定されることから、価格転嫁のあり方について協議が必要と促している。中小企業の負担軽減を図る観点から、サイバーセキュリティお助け隊サービス（新類型）での支援を強化していきたい。
- 本制度のコンサルティングサービスの営業活動が過熱しており、高額な委託料の支払いが★の取得に不可欠となる状況は、本制度の趣旨に反するものであるため、企業が自力で★を取得可能となる持続可能な制度設計が求められる。また、サイバーセキュリティお助け隊サービス（新類型）についても、より適正な価格設定が必要である。

  ⇒本制度は、外部コンサルティングに依拠せずとも自社において★を取得可能な設計となっているが、支援を要する企業についてはコンサルティングサービスの利用も想定されている。サイバーセキュリティお助け隊サービス（新類型）についても、適正な価格設定となるよう、努めて参りたい。
- 本制度の適用対象が明確でなく、部分的に★を取得できる仕組みが必要。企業全体という単位では大企業が★を取得できない懸念がある。

  ⇒★の取得単位については原則として法人単位を想定しているが、事業部単位での取得も考えられる。なお、現時点で単位については明確になっていないが、同じ IT 基盤であれば同じ評価であることが望ましいと考えている。この点、ガイダンス資料での明記を検討する。
- 内閣官房国家サイバー統括室（NCO）にて重要インフラ統一基準の検討が進められているが、重要インフラ事業者に対して、本制度の要求事項との関係性や整合性について明確に説明することが求められる。

  ⇒重要インフラ統一基準を検討している NCO も共同事務局として本検討に参画しており、NCO は経済産業省とも連携して検討を進めている。重要インフラ統一基準と本制度とでは目的が異なることを踏まえ、重要インフラ分野にとって過度に厳しい基準とならないよう両制度の整合性を考慮しつつ慎重に検討を進めていきたい。
- 重要インフラ統一基準と本制度の目的が異なる点は理解したが、遵守すべき基準が増えると負担が増えるため適宜考慮いただきたい。
- 本制度について 40 数社と意見交換を行った。そのうち2社からはこれ以上新たな制度を立ち上げないでほしいという意見があった。NCO でも重要インフラ統一基準を検討していると聞いたが、本制度と重要インフラ統一基準がつながっている点を認識いただきたい。
- 本制度は大企業よりも中小企業に重きを置いた上で、わかりやすい制度にした方がよい。ターゲットを大企業と中小企業で分けるのであれば、別途議論をすべき。
- ★4の要求事項を全て満たせていなくとも、次回に改善されていれば評価することが重要ではないかと考えている。セキュリティは継続して実施していくことが重要。★4を取得したとしてもサイバー攻撃を受けることがある。

- 経験上、評価者によって評価の品質等はばらつく。重要なサプライヤーに深刻なセキュリティインシデントが発生した場合、自動車を製造することができない場合も生じ得ると推察される。アナログでも事業を継続することが重要。
  ⇒評価者のばらつきをなくす取組は必要。ガイダンス資料や専門家への教育等でばらつきを減らす努力をしたい。
- 評価機関として活動したいと、一般財団法人日本自動車研究所(JARI)が名乗りを上げたが、心強く思っている。自工会では、「自工会・部工会サイバーセキュリティガイドライン」(以下、自工会ガイドライン)の他に説明資料を公開しており、よろず相談会も実施している。
- 自工会ガイドラインは継続的な更新、改善を行っている。本制度においても、要求事項及び評価基準の定期的な見直しをお願いしたい。
  ⇒IT全体の環境は年々変化していく。制度開始後も必要に応じて、変化を踏まえた基準、制度の見直しを進めていきたい。
- 発注者の立場から、取得希望企業が★4を取得しようとした際に不適合項目がみつかった場合、発注者側はその項目を知ることはできるか。
  ⇒発注者に対しては、取得希望組織が開示しない限り、評価項目に係る情報は開示されない。
- 資料に「原則として適用範囲に含めるが、例外的に適用範囲に含めないことが許容され得るもの」が示されており、例外を認める記載となっているが、その例外がリスクを招き得る。例外を認めている理由を明記したほうがよい。
  ⇒要求事項に対する適合もしくは不適合について、★4の取得希望組織は第三者評価機関からフィードバックを受けることになっている。必要に応じて、任意でフィードバックの内容を開示させることがあると考えている。
- 資料で「脆弱性管理体制、管理プロセスの明確化 [No.3-2-1]」が★4の要求事項及び評価基準に盛り込まれている。ただし、プロセスがあったとしても、そのプロセスが実際にワークしないと危険である。評価機関で確認いただきたい。もし、そのような評価基準となっていなければ、別添資料に追記いただきたい。
  ⇒今後チェックリストを作成する予定。評価判定の理由はセキュリティ専門家等が記載するものだが、例えば、適用範囲に含めないことを許容した理由を記載できる形等が考えられる。
- 地方の企業も、本制度に係る検討が進んでおり、一部の地方企業は戦々恐々としている。制度運用開始まで1年ほど期間があるため、地方での説明会も実施いただきたい。また、地方企業も制度を活用できるよう検討いただきたい。
  ⇒年明けから地域ごとに説明していきたい。また、来年度にサイバーセキュリティお助け隊サービス(新類型)の実証を予定。サイバーセキュリティお助け隊サービス(新類型)による支援を受けながら、地方の企業も含めて各企業が★を取得できるよう理解を促していきたい。
- 制度オーナとして IPA が示されているが、責任が全て IPA にあると認識されるとミスリードである。制度的な責任は政府が持っており、IPA がオペレーションを行う旨を明記した方がよい。責任分界について、政府を全面に出してはどうか。
  ⇒経済産業省が、本制度のスキームオーナーである IPA に対し責任を持って監督して参りたい。

以上