産業サイバーセキュリティ研究会
第12回 ワーキンググループ1（実効性強化・国際連携）
議事要旨

1. 日時・場所

日時：令和8年3月10日（火） 17時00分～19時00分

場所：オンライン開催

2. 出席者

委員　　：佐々木委員（座長）、渥美委員、上原委員、江崎委員、岡村委員、河野委員、中嶋委員、其山委員、高倉委員、三浦様(多田委員代理)、丹委員、古田委員、谷委員

専門委員　　：高柳専門委員、坂下専門委員、田中専門委員

オブザーバ　　：内閣官房 国家サイバー統括室、内閣府、警察庁、金融庁、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、デジタル庁

事務局　　：経済産業省 奥家大臣官房審議官、武尾サイバーセキュリティ課長

3. 配付資料

資料1 議事次第・配付資料一覧

資料2 委員等名簿

資料3 事務局説明資料

4. 議事内容（⇒部分は事務局による発言）

＜サプライチェーン全体のセキュリティ対策強化について＞

・ 基準やガイドラインを政府として示したのは大きな前進である。一方で、制度は実際に使われることで社会に実装され、目標を達成できるようになることが重要であり、活用方法や効果を段階的なステップとして示すべきである。制度そのものが前面に出すぎると受け手側のハードルが高くなるため、受け入れやすいところから段階的に広げていくことが重要である。

⇒御意見については、今後の政策の参考とさせていただく。

・ 制度の普及に関して、評価と課題解決のサイクルを継続的に回していくことが重要である。技術的に目標達成が困難な中小企業も多いと考えられるため、定期的な評価・課題解決のサイクルを回すことが必要であり、政府の役割に期待する。

⇒御意見については、今後の政策の参考とさせていただく。

・ SCS 評価制度に対して多くの企業が身構えている印象があり、求められる水準やスケジュール感を早めに示すべきである。また、社会における安全な状態についての共有概念を醸成するよう情報発信すべきである。制度の目的はセキュリティ産業の育成ではなく安全な社会の構築であることを再確認し、国際連携の重要性もアピールすべきである。

⇒SCS 評価制度については、そもそも★3・★4 の取得をどこまで求めるかについて、また IT 基盤を対象としているという点も含めて、講演などを通じて民間での普及を進めていきたい。産業界からも国際連携に関して要望をいただいており、それも踏まえて今後も連携の取組を進めていきたい。

・ SCS 評価制度や JC-STAR について、セキュリティ対策状況を可視化・評価できる共通の物差しが整備されたことは非常に価値がある。一方で、各制度の関係性や違いが分かりにくく、中小企業では制度体系の理解自体が負担とな

っている。SCS 評価制度と JC-STAR の混同も見られるため、制度全体の関係性を俯瞰的に示す資料や、各制度を使いこなせる仕組みの整備が必要である。

⇒わかりやすく説明しながら、制度の普及を進めていきたい。

- サイバーセキュリティお助け隊サービスの新類型について、従前の類型との違いを含め積極的に周知すべきである。また、中小企業のコストへの不安に対しては、成功事例をモデルケースとして周知することが効果的である。

  ⇒サイバーセキュリティお助け隊サービスについて、御指摘の新旧類型の違いを意識しつつ、今後も説明していきたい。価格感については、来年度の実証事業を通じて目安を示していきたい。
- 中小企業向けには、わかりやすい教育マテリアルの整備が求められる。OT 領域の認証制度やチェックリスト、クラウド事業者向け制度の充実も今後検討すべきである。また、地方企業とセキュリティ専門家とのマッチング事業にも期待する。

  ⇒SCS 評価制度については、来年度以降 IPA において、教育マテリアルも含めてガイダンス資料を整備する予定である。OT 領域については、各社で環境が大きく異なると考えている。まずは工場におけるセキュリティガイドラインの整備を検討したい。地方企業と専門家のマッチングについては、「中小企業向けサイバーセキュリティ対策支援者リスト」としてマッチングの仕組みを構築しているところである。クラウド事業者向けの制度の充実については今後の政策の参考とさせていただく。
- 各政策について横断的な一覧資料や、法令・ガイドライン対応のスケジュール感を経営者層に届くよう周知してほしい。政府調達仕様や欧州サイバーレジリエンス法への対応スケジュールの提示は、各企業の担当者が経営層を説得する材料となる。

  ⇒わかりやすい説明のために何ができるかについて検討させていただく。
- 「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構築促進に向けた想定事例及び解説」は大きな進歩であるが、認知度向上に向けた施策が望まれる。また、中小企業がセキュリティ対策をステップアップできるよう、税制措置やサプライチェーン上位企業への働きかけをお願いしたい。

  ⇒制度への対応のインセンティブに当たっては、今後政府調達要件の検討について、国家サイバー統括室と連携して進めていきたい。

＜セキュア・バイ・デザインの実践について＞

- 「セキュア・バイ・デザイン」への表記変更は、NIST や CISA と統一する意味で評価できる。この考え方には、ソフトウェア構成要素の可視化だけでなく、ゼロトラストアーキテクチャに基づく動的ポリシー制御による迅速な修正という観点も含めるべきである。

  ⇒国際的に「セキュア・バイ・デザイン」の呼称が一般的となってきていると認識しているため、今回の資料でも表記を統一している。また、ゼロトラストアーキテクチャに基づく脆弱性対応については、IPA 及び一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）との連携をさらに深めていくことなど、環境面を含めて政策を進めていきたい。
- JC-STAR の★1 取得で十分という誤った認識の広まりが懸念される。重要インフラ事業者では★2 以上が必要であり、戦略的な発信活動が重要である。

  ⇒JC-STAR について★1 では十分ではないという御意見には同意である。★2 以降も順次検討を進めていく中で、エネルギー業界からも★2 以降に対する期待が寄せられており、そのようなニーズも踏まえて制度を整備していきたい。
- スマートホームの JC-STAR★2 はユースケースごとに要件が異なり、デマンドレスポンスのような SWG 組織の隙間に落ちる領域がある。★2 の議論を進めるための場の整備と、レベル感のばらつきを防ぐ横串の議論が必要である。

  ⇒JC-STAR★2 のユースケースごとのレベル感に関しては、御意見を踏まえて慎重に検討していきたい。

・ 英国 PSTI 法と JC-STAR の相互認証は素晴らしい取組であり、相互認証の推進は制度普及に資する。欧州サイバーレジリエンス法との相互認証も加速すべきである。ただし、同法はハードローであるため、日本側も電気用品安全法等の関連法令を拡張して対応する必要があるのではないか。また、英国側からの使いにくさがないかも確認が望まれる。

⇒JC-STAR と PSTI 法との相互認証に関しては、御指摘のとおり JC-STAR が PSTI 法を完全に包含しているという関係性であり、どうしても片務的にならざるを得ないという状況である。英国側でも両制度の違いについては認識していただいている。なお、ハードローの整備については、今後の政策の参考とさせていただく。

・ SBOM の今後の動向について各業界への周知を進めてほしい。

⇒経済産業省では SBOM をめぐる課題の解決に向けた、「ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引 ver 2.0」を 2024 年 8 月に公表し、各種 ISAC などでも参考にしていただいている。個別の相談があればサイバーセキュリティ課まで御相談いただきたい。

＜その他（CPSF、PQC、AI関連等）について＞

・ PQC への対応は多くの企業が関心を持っている。2035 年までの対応が前提となっているが、準備に時間がかかるため前倒しで広報活動を進めてほしい。EU の研究機関からは PQC の次の枠組みに関する議論の打診もあり、研究面での先を見据えた検討も始まっている。

⇒PQC への対応に当たっては、ロードマップとして基本的には 2035 年を対応期限としている。量子コンピュータの技術的進展は不透明だが、諸外国でも 2035 年を目標として対応を進めているところである。当然リスクに応じて場合によっては期限を前倒しすることも考えられる。関係省庁と連携し、民間企業にも前倒しで方向性を示せるように、取組を進めていきたい。また、PQC への対応についてもその次を意識しながら検討していきたい。

・ CPSF の改訂については、単に時間経過のみに基づく見直しではなく、運用状況や効果の評価に基づく必然性のある見直しが重要である。海外連携については、日本発のガイドラインとして先導する気概を持って進めてほしい。

⇒現在の状況を踏まえながらアップデートしていきたい。また、CPSF は日本発の制度であるため、日本主導で海外連携を進めていきたい。

・ AI をベースにしたサイバー攻撃が当たり前になってきており、AI を使ったサイバー防御の検討が必要である。AI エージェントのセキュリティリスクへの取組は重要であり、営業秘密の漏えい等の観点からも検討すべきである。秘密情報の保護ハンドブックの AI 対応も望まれる。

⇒AIを用いたサイバー防御は経済産業省としても重要だと考えている。秘密情報の保護ハンドブックについても IPA と連携させていただく。

・ AISI と AI×セキュリティの取組との関係を整理すべきである。生成 AI など技術進歩のスピードが速い中、技術が世に出てからでは対策が間に合わないため、先読みして対策を先手で進めることが重要である。

⇒AISI との間では議論を進めており、具体的には AI の開発者側における評価ガイドを進めていく予定である。AISI とは引き続き連携していきたい。技術動向の先読みについては難しい局面もあるため、関係機関からトピックなどの情報連携をいただくなどして対応していきたい。

以上