サイバー・フィジカル・セキュリティ確保に向けた
ソフトウェア管理手法等検討タスクフォース
（第14回）議事要旨

1. 日時・場所

日時：2024年12月25日（水）10:00～12:00

場所：オンライン開催

2. 出席者

委　　員：土居委員(座長)、出雲委員、伊藤委員、稲垣委員、猪俣委員、大場委員、木谷委員、下村委員、
中嶋委員、髙橋委員、寺田委員、萩原委員、松岡委員、渡辺委員、野山委員

オブザーバ：厚生労働省、一般社団法人 日本医療機器産業連合会

事　務　局：経済産業省　商務情報政策局　見次サイバーセキュリティ制度企画室長
味木サイバーセキュリティ課補佐、飯塚サイバーセキュリティ課補佐

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 サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォースの検討の方向性

資料 4 SBOM の国際共同ガイダンスについて（委員限り）

参考資料 1　SSDF と国内ガイドラインのマッピング表（委員限り）

参考資料 2　SBOM の国際共同ガイダンス「フェーズ1」（委員限り）

参考資料 3　SBOM の国際共同ガイダンス「フェーズ2」案（委員限り）

4. 議事内容

事務局から、資料 3 と資料 4 に基づき説明した後、自由討議を行った。各委員からの意見は以下のとおり。

＜資料 3 について＞

●今後の成果物の方向性

- 例えば、SBOM が普及した際に、ソフトウェアやソフトウェアを含んだ製品を購入することは、SBOM 情報を購入することと同義になると考える。そのため、事業者の SBOM の管理等の取組に係るコストを適正に負担することが必要になると考える。さらに政府調達に SBOM を用いるとなると、会計法に従って適正な価格で競争性のある入札を行う必要があると考える。その際に基準価格の設定のためにどの程度のコストで調達することが適正かを検討する必要があると考える。これらのような現実的な施策を行うために実施できていないことも含めてまとめて頂くと良い。

- 資料 3 の p16 に記載されている SSDF の達成基準に関しては ISMS 認証制度のような PDCA サイクルの確認等が考慮されているが、実施している具体的な手段（管理策に相当する情報）の確認も必要ではないかと考える。

- 粒度が細かいが、SSDF が抽象的であるために包含できていない部分が具体的に5つあると考える。
  1 つ目は、「PO.2.1：役割と責任の定義」において、プロジェクト要員の教育について記載があるが、要員を集める段階で各個人に対するクリアランスの観点が必要だと考える。
  2 つ目は、「PO.5.1：開発基盤の分離および保護」において、データ保護も重要であり、本番データとテストデータを分ける必要があると考える。特に、個人情報等の重要な情報を開発環境に利用することの是非やアクセス権限の管理等が求められるとよい。
  3 つ目は、「RV.2.2：脆弱性に対するリスク処置の決定と対応計画および実施」のリスクの深刻度の判定において、脆弱性のみを見て判断してしまう懸念があると考える。重要な情報資産につながる脆弱性に関しては CVSS が低くても対応するなど、対応の優先度付けの判定基準には注意を払う必要があると考える。
  4 つ目は、「RV.3.3：類似の脆弱性の積極的な検出」において、Microsoft が公表していたとおり、CWE を元にした手法の紹介を検討できると良いと考える。
  5 つ目は、リリースするプログラムにデバッグ用のコードや仕様にないモジュールが残存していると脆弱性につながる可能性があるため、不要なコンポーネントを SBOM で検出できると良いと考える。

- 1 つ目についてだが、要員のクリアランスを求めるには、日本の文化的な観点から個人情報などに敏感であり困難であると考える。

- 国内ガイドラインを SSDF へマッピングすることは賛成である。ただし、包含関係の「◎」に関しては再度検討できると良い。例えば資料 3 の P20 に書かれている、SSDF の PS3.1 と CPSF の IP-4 のマッピングに関しては「◎」というよりは「○」か「△」が妥当と考える。SSDF の PS3.1 ではソフトウェアリリースの完全性検証情報等を安全に保管するといったタスクであるのに対し、CPSF の IP-4 は定期的なバックアップといった対策要件となっていると認識している。データを保存するという観点では同じかと思うが、保存するデータに関しては同等以上とは言い切れないのではないかと考える。こういったミスリードはクロスリファレンスに原因があるのではないかと考える。CPSF の対策要件を満たしている事業者が SSDF への対応を行う際に、「◎」と記載されていると対策を行わないといった事例も考えられ、「◎」の評価に関しては再度検討が必要だと考える。

- SSDF は大統領令が出た段階で改訂されていると認識している。マッピングの中で改訂前後における齟齬を埋めていく取組ができると良い。

- 導入ガイダンスの基礎編など国内関係者が現実的に取り入れることが可能な取組に関しては賛成である。国際的な取組により国内の事業者が振り回されないようにして頂けると良い。SSDF に限った話ではないが、対応の優先度付けに関しては課題が残っているので議論が必要であると考える。

- 今回のマッピング等には賛成である。SSDF 実証の事例数に関しては増やしていくことは必要であると考える。また、業界団体の会員で同様の実証を行った場合、対応レベルが低くなることが想定される。そのため、各社が SSDF を考慮できる段階までに持っていくといった何らかの支援が必要となると考える。中小企業のベンダーの負担が増える可能性もあるため、そういった面を考慮しながら今後の方向性を検討頂けると良い。

- SSDF のタスクに関して経営陣の関与の記述が薄いと認識している。経営層の関与についてもっと強調すべきと考える。暗号分野でも経営層の関与を行う方向性としていると認識している。

●今年度以降の事業について

- 政府調達の要件化等を考えると、今後の課題として、「サプライチェーンにおける責任の問題」「脆弱性情報の最新状態の維持のための体制」「国際競争力確保のための情報収集体制」「サプライチェーン上のコスト転嫁の仕組み」を入れて頂きたいと考える。重要インフラのサイバーセキュリティに係る行動計画の中でサプライチェーンのセキュリティ対応を行うことが求められている認識だが、コスト転嫁や責任が明確でないとずさんな情報管理となり、施策として成立しないと考える。何を行えば皆の役に立つかの議論ではなく、次のフェーズとしては具体的にステークホルダー、実施内容、役割と責任、コスト負担などを議論できると良い。また、国際的な協調も考慮して日本の施策を検討する必要があると考える。このような検討が行える体制が敷かれているかを検討できると良い。他国の制度を真似しているだけでは、独禁法や下請法などの法的課題が出てくると考える。今後の検討に掲載されているものもあるが、具体的な姿が見えてこないため、検討できると良い。

- 米国では政権移行に伴い、政策の動向に変化がある可能性がある。具体的には、一般教書演説から落とし込まれていくことであるが、今後の SBOM を担当する部局や QUAD のような複数国の枠組みに関しての動向に関しても見極めていく必要があると考える。規制・技術上の垣根を他国と作らないことが重要であると考える。少なくとも日米間では平仄（ひょうそく）を合わせると良い。

- 脆弱性のハンドリングに関して、ソフトウェアを提供する会社にとってメリットがある形にしないと SBOM は普及しないのではないかと考える。メリットとして脆弱性情報を提供することも検討できると良い。

- SSDF を実施することは相当難しいと考える。特に、中小企業でセキュアなソフトウェア開発を実施するための施策等を考えていくうえで、中小企業のセキュアソフトウェア開発のレベル感の調査が必要であると考える。ガイダンス等の提供の前に、業界団体などを通じてどういった課題感やニーズがあるのかを把握頂けると良い。

- 規模の大きい企業であっても PSIRT が存在する企業は多くないと認識している。これが実情であると考えると、SSDF が現実的なものなのかを考えていくべきであり、実態も含めて調査できると良い。また実装のコストや実装に向けて相談するステークホルダーがどこにあるのかは明確にして頂けると良い。

- 調査の面では、国際的な調査も行って頂けると良い。コスト負担のあり方というのは国際競争力にも影響するので、どういう仕掛けでどういったコスト負担を行っているかを調査頂けると良い。それから情報について虚偽の情報があった際の責任についての動向についても調査頂けると良い。

- 今後作成予定の SSDF の導入ガイド基礎編の普及は、政府調達の要件とすることを検討するのであれば、早い段階で普及できればと考える。ガイドは業界団体等を通じて紹介頂ければと考える。

- 生成 AI によるコード生成に関して知財面の課題があると考える。SSDF 導入ガイダンスの応用編では生成 AI の自動生成コードの管理に関して踏み込んで整理頂きたいと考える。

以上