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15回）議事要旨

1. 日時・場所

日時：2025年3月4日（火）13:00～15:00

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、木谷委員、下村委員、高田委員、
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：内閣官房内閣サイバーセキュリティセンター、警察庁、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 サイバーインフラ事業者に求められる役割等の検討会について

参考資料 1 セキュア・ソフトウェア開発フレームワーク（SSDF）導入ガイダンス案（中間整理）

参考資料 2 SSDF 導入ガイダンスタスク整理シート

参考資料 3 11.付録 SSDF 導入の実証例

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。各委員から意見は以下のとおり、

＜資料 3 について＞

●<u>今年度の成果物について</u>

- SSDF の具体化に伴い、例示された対策のみ実施すれば良いと受け取られてしまう可能性があると考える。例えば、今回の資料においては、タスクのレベル 1 は例として中小企業向けとしている内容があると理解した。PO1.1 のタスクレベル 1 で任意としているテスト環境について、任意を理由に中小企業が対策しなくても良いと誤解してしまう可能性がある。本来 SSDF を元に主体的に考えてもらうことが望ましい。そのために検討いただきたい点が 2 つある。
  - 1 つ目は、各タスクに検討すべき観点や実施しない場合のリスクを列挙することが考えられる。CVSS のみならず、自社へのシステムの影響を考えると良い。経営者や顧客サポート等の観点を含めることができればなお良い。
  - 2 つ目は、達成レベルに関して、項目として内容的な部分のレベル分けの観点も必要と考える。例えば、ポリシーの文書化の項目において、文書化がセキュリティとしての効果を高めるわけではないので、深さに関する観点を追加いただけると良い。また、システム全体に対して対策を実施するか、システムの一部に対策を実施するか

などの広さの観点でもレベル分けをしていただけると良い。資料 3 の P12,13 に関してはプロセスの成熟度とリスクといった別の観点での記載がなされていると考える。

- 成果物のまとめ方に関して検討いただけると良い点がある。参考資料 1 では会計監査における原則主義アプローチ（comply or explain）を採用するとあるが、SSDF を適用する場合に大企業においても未実施の項目が多いと考える。そのため、explain のみが実施され、安易な説明が行われる懸念があり、アカウンタビリティベースアプローチの有効性が揺らぎかねないと考える。解決策として、explain としてどういった説明を行うべきかといった想定例を記載できると良い。具体的な対策実施時期や代替案の提示といったような妥当性の説明に関する例を記載いただけると良い。

- 説明責任という言葉の意味や趣旨が多様的であるために難しいと感じる。リスクベースアプローチからアカウンタビリティベースアプローチに変わった場合の趣旨の差分を示すべきと考える。リスクベースアプローチからアカウンタビリティベースアプローチへの変化は自社のセキュリティ対策の合理性ではなく、相手との関係で契約に従い、誠実になることが重要となると考える。しかし、一般的には分かりにくいため説明が必要となると考える。

- 会計監査における原則主義アプローチの考え方が、今回のアカウンタビリティベースアプローチに合うかどうかは検討が必要かもしれないと考える。監査等の専門家が対応を行う分野の言葉を使うことは様々な解釈が生じる可能性があると考える。アカウンタビリティアベースプローチ自体は合理的で良い考え方だと理解しているため、会計監査における原則主義アプローチを用いず、分かりやすい言葉で説明いただけると良い。機能安全のアシュアランスケースに関しても同様の事項があると考える。

- SSDF の内容で、例えば RV3.1 の脆弱性の根本原因の分析など、難易度の高いものが掲載されている。難易度の高い項目に関して、できて当然といったメッセージにならないように注意いただけると良い。

- SSDF とは別に NIST SP800-216（Recommendation for Federal Vulnerability Disclosure Guidelines）の資料がある。米政府へシステムを納品する際に SSDF の Self attestation を実施することになるが、脆弱性情報は開示しなければならないため、SP800-216 に準じる形で脆弱性を開示する手続を取ると理解している。それに関しては SSDF 単体でハンドリングするわけではないと理解しているが、従来の JPCERT の枠組みを拡張する形で検討を行うのか、別の形で検討を行うのか考えていただけると良い。

- SSDF の和訳に関して、「プラクティス」を実践策、「タスク」を課題とするのには違和感があるため、今後も検討できると良い。

- NIST SP 800-218 におけるプラクティスはカテゴリとしての要素を含めたプラクティスであり、タスクはプラクティスの具体策や項目ではないか。

- SSDF の和訳に関しては国語学者等にも意見を伺うべきと考える。その国特有の文化を知らずに外国語を引っ張ってくるというのはユーザーに責任を押し付けてしまう可能性があると考える。

- 難しいかもしれないが、この機会に国内ガイドラインの用語を整理してはどうか。

- 用語の改訂や整理が必要な時期に来ていると思われる。SSDF の他、CISA SBD の用語との関係整理も有用。

・ 資料 3 の P3 において、SSDF を参照する形で Shifting the Balance of Cybersecurity Risk 文書が記載されている。ソフトウェア業界全体がどういった方向に向かうかに関しては Shifting the Balance of Cybersecurity Risk 文書に記載されていると理解している。その文書においては、セキュアなソフトウェア開発ライフサイクルに関する記述の中で SSDF を推奨する形になっていると理解している。Shifting the Balance of Cybersecurity Risk 文書との関係がわかるように明示いただければと考える。Shifting the Balance of Cybersecurity Risk 文書に関しては NISC が署名していることもあり、国内での認知度もあると考える。そのため Shifting the Balance of Cybersecurity Risk 文書からどういった取組が行われるかを示すことで全体が見えやすいと考える。

●今年度以降の事業について

・ 広報や普及促進策については、認証制度の準備が検討予定とされているものの、完成するまでには時間がかかると考える。本認証制度を必ず利用しなくても、自己適合宣言の形で表示する案も考えられるが、そうでなくても自分自身で「SSDF に準拠しています」や「その一部を実施しています」といったことを示すことが大切だと考える。取引先に対する表示の方法についても検討することが、特に中小零細企業にとって重要となり、説明責任を果たすことが難しい場合、どのように対応すべきか検討する必要があると考える。製品開発の際に、SSDF への適合性を表示・宣言した場合、その内容が品質とも関係し、契約の一部として効力を持つと考える。そのため、問題が発生した場合に取引先に対して SSDF に関する実施状況を説明する責任が生じると考える。したがって、認証を取得していることや、その表示方法も契約内容になると考える。SSDF の適合性を表示していくことが、利用する際に便利で良い取組になると考える。

・ 米国の産業界の状況について、義務の程度や導入のスピード感など、新しい政権における方針をさらに注視していく必要があると考える。日本だけが先行してしまうと、日米間でギャップが生じる可能性があるため、連携できる事項や相互の投資関係などについても、調和を図ることが重要だと考える。

・ SSDF については、政府調達での活用が考えられるが、政府調達以外に浸透させる場合にどのレベルを求めるのか、緩和策等も含めて検討できると良い。政府調達以外への浸透も検討するのであれば、目的やスタンス等も設定し、明示することも検討できると良い。

・ 政府調達での活用に関して、レベル設定の段階で海外と差異が出てしまうことがないように検討できると良い。

・ レベルが設定されている場合、調達の基準としての使われ方が想定されるが、一方で、本来のモチベーションとしては、あるレベルを超えることにより、安全性の向上等が狙えることを示すべきであると考える。そこで重要なのは、自ら考え、必要な対策を選択するという観点を提示し、その観点に基づいて選択した対策が具体的にどう安全性や準備に役立つかを明確に示すことだと考える。現状のレベル 1 には難易度の高いものがあるため、今後の実証において具体的にどの項目が実行可能であり、どの項目が負担となるかを見極めるべきであると考える。

・ セキュアであるということがその企業等への信頼につながる、といった感覚をセキュリティ関係者以外の人たちも含めて共有できないと、SSDF を利用する目的が調達等に引っ張られてしまう恐れがある。

・ 次年度として、モデルケース等を設定して SSDF の利用ケースやどういったリスクを抑えられるかを可視化できると良い。

- 政府調達に関連して政府がガイドラインや基準を公開する場合、政府機関に限らず、民間企業にも責任が伴う。そのため、(SSDF 実装のためのレベルの記載が)あくまでも例示であるのであれば、ガイドラインの使い方について説明を記載したほうが良い。例えばコンサルティングが行われる場合、「政府がこう言っているからこれは必須だ」として、レベル 1 の適合も難しい状況であることを本アウトプットを出すときに理解しておきながら、適合を求める可能性があると考える。レベル 1 でさえも難しい場合があることを明記するなど、ガイドラインの正しい使い方をしっかりと記載する必要があると考える。

- SSDF やその他のガイドラインがしっかりと浸透するためには、SSDF の内容をきちんと学ぶ場を提供することが重要であると考える。業界団体や開発企業、SIer などを含めた勉強会やセミナーが必要となると考える。

- 自己適合宣言の整合性についても重要であり、Security Action や JC-STAR などの既存の取組とバランスを保つことも必要となると考える。

- 現場の意見としてはツールチェーンが気になるため、具体的に検討すると良い。

- 政府調達において民間製品を多く使用している現状を考慮すると、「政府調達に限る」という制限を設けるべきではなく、民間全体での導入を目指すべきであると考える。そのためには、政府だけでなく、民間の取引が SSDF の基準を尊重し、利用可能な状況を作ることが求められると考える。また、経済合理性を持たせ、自然と普及していく環境を整えることが大切であると考える。強制的な法律は最後の手段とし、経済が循環する形での普及を目指すアプローチが理想的だと考える。

- ビジネスの課題であると経営陣が認識しなければならないと思うが、なかなかうまく行かない。米国大統領令含め昨今の欧米の規制や義務化の流れは、他に短期的に実現する手段が無い事を示しているように思える。日本政府としてどのように実現するかについては、自主性に任せるだけでは課題が多いと感じる。

- Secure by Design の観点で、特にビジネスプラクティスの結果を公表することや、ソフトウェア開発ライフサイクルの良い事例や悪い事例を記録として活用することは、非常に有意義なアプローチとなると考える。今回の SSDF においても、具体的な事例を挙げることで、実際の取組に即したガイドラインを構築することが可能となると考える。具体的な事例を集めて提示することは、Secure by Design が求める必須事項とも合致し、実効性のある普及策に繋がると考える。実際の開発現場での成功事例、失敗事例を蓄積し、それを基にしたフィードバックループを作ることが、今後の改善や新たな取組の指針になると考える。

以上