

産業サイバーセキュリティ研究会WG 1
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16回 議事要旨

1. 日時・場所

日時：令和7年7月30日（水）13時00分～15時00分

場所：オンライン開催

2. 出席者

委員：土居委員（座長）、青木委員、出雲委員、伊藤委員、稲垣委員、木谷委員、黒坂委員、
下村委員、高田委員、高橋委員、寺田委員、萩原委員、松岡委員、渡辺委員

オブザーバ：警察庁、デジタル庁、外務省、厚生労働省、防衛省、
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 橋本企画官、大久保課長補佐、関戸係長、
株式会社三菱総合研究所

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 ソフトウェアの安全な利活用に関する海外の動向

資料5 本年度の調査・実証の進め方（詳細）

4. 議事内容

○事務局から、資料3、4及び5について説明を行った。

○各委員から、主に以下の意見があった。

＜本年度の調査・実証の進め方について＞

- ・ 実施事項やツールの使い勝手を、実証を通してチューニングすることが重要であると認識している。供給側の目標は、コンテンツが多く利用されることであるため、実証調査では利用者側の立場で、コンテンツに関する意見や使用環境をどのように改善すればよいかについて、情報収集することが望ましい。
- ・ 実証のスコープについて、例えば金融機関では様々な開発手法が導入されており、すべての開発手法について実証を行うことは困難であると思うが、現実に応じた実証を実施いただきたい。また、SBOM及びSSDFは、国際的なルール、監査ルール等を含めた金融機関を統制する他のルールとの整合性を図ってほしい。
- ・ SSDFは非常に範囲が広く、実施に係る労力が大きい。SSDFを実現することは、アプリケーションセキュリティを実現することと同義である。サプライチェーンの中でSSDFをベースにセキュアな

製品を組み立てることは、大手メーカーは可能であっても、末端でソフトウェアを提供している小規模事業者は難しいのでは。その背景には、コスト、技術、リソース及びノウハウの問題がある可能性が高い。最終製品の中には中小企業のコンポーネントが組み込まれることが多く、本取組のスコープとしてカバーしなければならない。中小企業でSSDFを導入するために、ツールの使用経験や人材の足りていない組織での実証や導入支援プログラムも必要と考える。

- ・ SSDFに準拠する際、発注者が受注者のどちらかがコストを負担する。その際のコストとして妥当な金額の目安が公開されていれば、中小の受託会社は契約額の増分を主張できると考える。例えば、SSDFに準拠せずに開発した際の費用がいくらで、SSDFに準拠して開発した際の費用がいくらであったといった事例があるとよい。SSDFに準拠するためのベースとなる体制を作るにはどれだけのコストが必要かを明らかにすることで、体制整備等に対して補助金を交付するという議論にもつながる。
- ・ 生成AIの進展により、ローコードツールやノーコードツールを使用しなくても、誰もがプログラムの生成を行えるようになってきた。生成AIは、インターネットに公開されているオープンソースソフトウェア(OSS)のソースを学習することで、プログラミング能力を高めているとされている。一方で、脆弱性のあるコードを生成AIが出力してしまうことが多く指摘されている。その原因の一端は、学習対象となっているコードに脆弱性が含まれていることにありと考えている。ある意味では、学習対象となるOSSのコードをSSDF対応にする必要がある。SSDF for AIという発想。AIを活用することが、良質なソフトウェアを基に開発することと同義となるように、まずはOSS開発者へのSSDFの啓発等を検討することも一案と考える。
- ・ 補助金等の枠組みにより、中小企業がSSDFを担保するためのコストを負担できる仕組みを検討してもらいたい。オープンソースのツールでは不十分な場合も当然存在する。そのため、実証において効果の高いツールの組合せ方が明らかになれば、当該ツールの組合せを導入するためのコストを経済産業省が担保することが望ましい。
- ・ AIが社会、特に開発の現場でどのように使用されているか、現在の状況をまず国内で調査してもらいたい。調査結果に基づいて、採るべき指針は変化すると考える。
- ・ リソースの格差を乗り越えるために、ツールの情報は重要である。また、モチベーションの確保や対策の必要性の伝達のために、SSDFのタスクを実施しないことによるリスクを明確化して、コミュニケーションすることも重要と考える。その上で、自己チェックリストを使う際に、チェックする担当者の感じる課題点や懸念点等の細かな声を吸い上げる仕組みが存在し、当該の内容がフィードバックされることが望ましい。
- ・ IT導入補助金の対象となるツールにソフトウェア管理ツールが含まれると、円滑に経済産業省の枠組みの中で補助金の交付が可能となるのでは。ひとつのアイデアとして受け止めてもらいたい。
- ・ SSDF及び関連するガイドラインは、地域のSI事業者等にはあまり浸透していない。認知度に関する、現場の立ち位置や財務的な制約を考慮した投資可能額等についての質問調査を実施して、現状を把握し、その結果を踏まえてプロモーションについて議論することが望ましい。

- ・ チェックリストの利用は有効であると認識しているが、ソフトウェアを提供する会社は、様々な負荷が重い対応を実施しているため、全体感を踏まえた認証の統一や差分認証を視野に入れた調査研究を行ってほしい。また、省庁等の政府機関がチェックリストを守れるかも論点となる。
- ・ SSDF、SBOM等は、各事業者がISO/IEC 27000シリーズに準拠した取り組みを行うこととは異なる性質を有する。中小企業が補助金を交付されても、SSDFの導入は限定的な範囲に留まると考える。大小を問わずベンダーは世界も相手にしており、本当に役に立つという確信がない限り、ルールは定着しない。ルールを実施せよと命じればあらゆる事業者が実施するという発想からの転換が必要。ISO/IEC 27000シリーズですら、定着までに数十年の時間がかかり苦労を要した。
- ・ 中小企業がツールを使用することを想定すると、コストだけでなく、グローバルで通用するか、国産であるかなど、ツールの選定基準も論点となる。例えば、工数削減の効果の高いツールを選ぶという趣旨がある場合は、その旨の記述が必要。様々な可能性を踏まえて、どのような母体や選定基準でツールを選定したのか明らかにするとともに、ツールに関する不満点やあるべき仕様を調査で明らかにすることができれば、当該情報を開発ベンダーのイノベーション促進のために活用できると考える。
- ・ 中小企業におけるセキュリティ対策の底上げという観点から考えると、SSDFは、どのような対策をどの程度まで実施するかを議論するための材料となる。発注者と受注者の間で、実施事項や考慮事項を相談する際、SSDFベースで確認することになる。サプライチェーン全体又は会社全体という規模で対策を実施する場合は、コスト及び負担が大きくなるので、まずはプロジェクト、製品又はサービスの単位で実施事項を議論して効果を確認することもひとつの方策と考える。
- ・ 生成AIについては、バンプコーディングと呼ばれる手法の登場により、品質を担保しないのであればプログラムの量産が可能な土壌ができています。一方で品質を担保するには、既存の開発手法と同様にレビューポイントを設けて人がチェックすることが必要であると、一般社団法人情報サービス産業協会（JISA）の勉強会で議論した。勉強会の中では、プロンプトの調整によって品質向上を目指す取組も実施した。生成AI自体の成熟に伴い、利用者の開発手法や契約形態等に様々な変革が生じる可能性を踏まえ、JISAがまとめた提言もあるため参考にしてほしい。
- ・ サプライチェーンやメンテナンスの領域においてSSDFの適用対象となり得るソフトウェアについて、分かりやすく伝えていかなければならない。現在の議論では全てのソフトウェアを対象としているが、例えばカスタムアプリ（システムインテグレーションで開発した業務アプリケーション等）については、自社内で使用するものと顧客に提供するものとの間にも違いがある。
- ・ AIに関しては、システムの重要な部分の脆弱性を検査するためのAIエージェントを強化する取組に対し、国として支援を検討することが望ましいのでは。

<取組の全体像について（次年度に向けた論点）>

- ・ 先行して取り組みを成功させている海外の事例について、なぜ成功しているか、環境、金銭の流れ、能力等に焦点を当てて情報を得たい。

- ・ 政府調達等での要件化等ではなく、自己チェックリストの検討とするのは、米国の取組の後退が背景にあると理解している。しかしS S D Fを普及させるためには、政府調達での要件化が効果的ではないか。自治体等も含めた政府調達により、地方のS I 事業者等への普及が進むと考える。導入の仕方の塩梅は論点であり、いきなり高いハードルを課すとハレーションを起こすため、比較的低いレベルから開始することが効果的ではないか。
- ・ A I－S B O Mに関する国際的な議論と国内の議論の整合性について注視することが望ましい。

以上