産業サイバーセキュリティ研究会ＷＧ１
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１７回　議事要旨

１．日時・場所

日時：令和８年１月２２日（木）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、猪俣委員、大場委員、木谷委員、黒坂委員、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

オブザーバ：内閣官房国家サイバー統括室、警察庁、厚生労働省、防衛装備庁、一般社団法人 日本医療機器産業連合会

講　演　者：株式会社エーアイセキュリティラボ　青木代表取締役社長

事　務　局：経済産業省商務情報政策局サイバーセキュリティ課　橋本企画官、大久保補佐、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】ＳＳＤＦガイダンスのあり方について

【資料５】ＡＩを活用したＳＷ開発への対応に関する有識者講演資料（委員限り）

参考資料１　ソフトウェアの安全な利活用に関する海外の動向

参考資料２　セキュア・ソフトウェア開発フレームワーク導入ガイダンス案（委員限り）

参考資料３　セキュア・ソフトウェア開発フレームワーク導入ガイダンス付属ツール等（案）（委員限り）

４．議事内容

〇事務局から、資料３及び４について説明を行った。

〇株式会社エーアイセキュリティラボ　青木代表取締役社長から、資料５について説明を行った。

〇各委員から、主に以下の意見があった。

＜ＳＳＤＦ導入ガイダンス案に対する改善案について＞

・　ＳＳＤＦ導入プロセスでは様々な段階で分散的にツール導入プロセスが実施される可能性があるのではないか。また、ＳＳＤＦのＲＶ．２．１の「脆弱性情報の収集と分析の実施」に対応するツールカテゴリとしては、ＳＢＯＭ管理ツールだけでなく、ＳＢＯＭに非対応の脆弱性データベース検索ツールやセキュリティーレポート情報収集管理ツールなども含まれるのではないか。

・　参考資料２の「セキュア・ソフトウェア開発フレームワーク導入ガイダンス案」において、対象読者の項に具体的な想定読者・組織を指定することが望ましい。

・　既に関連分野の前提知識を有している人がツールについて学習する場合、学習時間が抑制できる可能性がある。この点を踏まえてツールの学習時間の目安を提示することが望ましい。

・　ＳＳＤＦのタスクを担う主体を整理するにあたって、「技術者」を「開発者」「インフラ構築者」「セキュリティ技術者」等に細かく区分することが望ましい。

・　環境構成管理ツールの紹介にあたり、ツール利用時のイメージが湧くようになるよう、Ａｎｓｉｂｌｅのプレイブックや Ｄｏｃｋｅｒｆｉｌｅのベストプラクティス等を参考情報として合わせて記載するよう改めることが望ましい。

・　国内ガイドラインにおける不足事項への対応策の提示にあたって、米国では規定されていない、より厳格な項目が日本で規定されてしまうと、日米の平仄が合わなくなってしまうおそれがある。十分な検討が必要。

・　ＳＳＤＦで利用できるツールには条件付きで、無償で使用できるものがあるため、その旨を記載しておくことが望ましい。また、中小企業の導入支援において、有償の方がサポート体制等の面で有益である場合もあるので、その旨も言及することが望ましい。さらに、中小企業は当初からツールチェーンを一括で導入しない場合があることも想定されるため、個別のツールの組み合わせの事例等が紹介されているとより有益と考える。

・　ＳＳＤＦのタスクを実施しない場合のリスクとして、プラクティス単位でキーワードだけを抽出した一枚の資料があると、ＳＳＤＦによってリスクがどのように改善されるか一目でわかるようになると考える。

＜ＳＳＤＦ導入ガイダンスの活用策＞

・　米国のＳＳＤＦは米国の政府調達のために作成されたガイドである。日本においても、ＳＳＤＦ導入ガイダンスについて日本の政府調達で実証することが適切であると考える。

・　米国や欧州では、政府が資金を拠出して作成させたシステムやソフトウェアは、政府調達とすることが一般的。日本においても、政府が資金を拠出したシステムやソフトウェアは政府が率先して利用すべき。

・　金融機関は、現在金融庁のガイドラインへの対応を優先して実施しているため、ＳＳＤＦについては金融庁のガイドラインとの対応箇所から実施を進めてもらうことが望ましいと考える。

・　政府調達におけるＳＳＤＦの活用は是非進めてもらいたい。

・　プロモーションの一環として、企業が自己適合チェックを簡易に実施できるウェブサイトを作ってはどうか。

・　政府調達においては、省庁がシステムやアプリケーションの調達に伴う入札を実施する際に、ＳＳＤＦに準拠している入札者に対して加点することを検討するとよい。

・　近年は多様なガイドラインが公表されており、ガイドライン間の関係についてマッピングなどは提供されるものの、直ちに明らかではない場合もあり、困惑している人は多い。更に体系立ててガイドライン間の関係を整理することが必要な時期が到来しているのではないか。

・　構造的制約やリソース不足によってＳＳＤＦへの対応が後回しになってしまう事象は、往々にして発生する。特にリソースが不足している事業者におけるＳＳＤＦの普及及び実装を進めるためには、完璧な実装を要求せず、レベル分け等を設定することが有効。スモールスタートを実施するための最低限度の基準を設定することも一案である。

・　ＳＳＤＦ等に関連する仕組みや政策等の対象として、政府調達を実施するようなかっちりとしたシステム開発物が想定されているように感じる。対象としてどのような開発物を想定するかは論点であると考える。

・　ＳＳＤＦの普及に関しては、事業者がＳＳＤＦへの対応の達成度を他者にアピールできるようにする必要があると考える。

・　社会実装を進めるためには契約や合意が必要であるが、それらの概念について、ガイダンスでは具体的かつ詳細に解説されていないため、次年度以降具体化する作業を進めてもらいたい。また、テーラリングができる人材を育成することについても検討してもらいたい。

＜次年度以降の取組について＞

・　ＡＩ駆動開発に係るセキュリティに関する検討は、ＡＩそのもののあり方にもかかわる論点を扱うものと承知している。そのため、ＡＩ関連の政策を立てている部局とも適切に情報共有しながら作業を進めていくことが望ましいと考える。

・　ＡＩ駆動開発は、システム開発の効率化や省人化といったポジティブな側面だけでなく、開発者の裾野を大幅に広げ、脆弱性のあるソフトウェアが大量に頒布されてしまうというネガティブな側面もある。技術面だけでなく政策面でも様々な手当てが実施されることが望ましい。

・　ＡＩ駆動開発に関する検討が重要であることは理解するものの、継続検討が必要とされていたプロモーションを優先して実施すべき可能性があると考える。検討の内容を拡張していくよりも、ＳＢＯＭの普及策に焦点を当てるべきではないか。

・　狭義の開発だけでなく、関連する開発・運用・検査等の各フェーズにおいてどのようにＡＩが活用され、どのような課題があるのか、概観の整理をすることが望ましい。

・　昨今の生成ＡＩの悪用の事例を鑑みると、生成ＡＩは誰でも悪用できるという状況を前提として、悪用への対策をルール面と規則面から論じていくことが求められるのではないか。

・　ＡＩ駆動開発については、多くのレポートで指摘されているところではあるが、品質を担保するための仕組みについての調査及び実証が必要ではないか。

以上