経済産業省

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

令和７年７月30日

商務情報政策局サイバーセキュリティ課

議題

1. **ソフトウェアの安全な利活用に関する海外の動向 【説明：三菱総合研究所】（資料４）**
2. SSDFの活用促進に向けた取組の全体像【説明：経済産業省】（資料３：本資料）
3. 本年度の調査・実証の進め方 【説明：経済産業省】（資料３：本資料）
4. 本年度の調査・実証の進め方（詳細） 【説明：三菱総合研究所】（資料５）

議題

1. ソフトウェアの安全な利活用に関する海外の動向 【説明：三菱総合研究所】（資料４）
2. **SSDFの活用促進に向けた取組の全体像【説明：経済産業省】（資料３：本資料）**
3. 本年度の調査・実証の進め方 【説明：経済産業省】（資料３：本資料）
4. 本年度の調査・実証の進め方（詳細） 【説明：三菱総合研究所】（資料５）

SSDFの活用促進に向けた取組の全体像

- 米国国立標準技術研究所（NIST）の「セキュア・ソフトウェア開発フレームワーク（SP800-218 Secure Software Development Framework（SSDF））」を実践するための具体的な方法や手順等をまとめた国内事業者向け文書を策定するとともに、自己適合宣言の仕組みを構築し、政府調達等での要件化を通じて実効性を強化することにより、QUAD共通原則を履行することが目標。
- 昨年度は、SSDFの導入効果等の実証を行ったうえで、国内事業者向け文書の初版案として「SSDF導入ガイダンス案（中間整理）」を作成。本年度は、産業分野毎の実態に即して効果的にSSDFを導入・実践できること等を目的に複数分野における調査・実証も行ったうえで、ガイダンス案の拡充・成案化などSSDF導入促進に向けた取組の検討を進めて参りたい。
- なお、自己適合宣言の仕組み・政府調達等での要件化等については、今年度は国内事業者向けに自己チェックリスト（第三者による管理・運用を伴わないもの）を検討する。その上で、QUAD共通原則の履行との関係を踏まえつつも、政府調達での活用のあり方については米国の政策動向等も踏まえ今後検討して参りたい。

昨年度の取組（成果物）

- SSDF導入ガイダンス案（中間整理）
  - ✓ SSDFの概要
  - ✓ SSDF導入の意義・メリット、考え方、プロセス(自己適合宣言書の作成に関する参考情報を含む)
- （付録）SSDF 導入ガイダンスタスク整理シート
  - ✓ SSDFタスク達成レベルと具体的な実践策
  - ✓ SSDFとソフトウェア・セキュリティに係る既存の国内ガイドラインのマッピング　等

本年度の取組（案）

- 調査・実証を踏まえたガイダンスの拡充
  - ① ツール等を活用した効率的な導入・実践策
  - ② 分野特性に応じた活用策
  - ③ 達成プラクティスレベルの段階数の見直し検討
  - ④ タスクを実施しないことのリスクの明確化
  - ⑤ 国内ガイドラインの不足事項への対応策の提示
  - ⑥ 自己チェックリストの検討・案の提示

来年度以降の取組（想定）

- 調査・実証を踏まえたガイダンスの拡充（最新の国際動向等に対応した更新、代表分野に対応したガイダンス（応用編）や中小企業等にも活用いただきやすいガイダンス（簡潔版）の作成 等）
- 業界団体との連携を通じたガイダンスの普及促進策の検討
- コスト負担の在り方検討　等

議題

1. ソフトウェアの安全な利活用に関する海外の動向 【説明：三菱総合研究所】（資料４）
2. SSDFの活用促進に向けた取組の全体像【説明：経済産業省】（資料３：本資料）
3. **本年度の調査・実証の進め方 【説明：経済産業省】（資料３：本資料）**
4. 本年度の調査・実証の進め方（詳細） 【説明：三菱総合研究所】（資料５）

本年度の調査・実証の進め方（案）

調査・実証の成果目標

① **ツール等を活用した効率的なSSDFの導入・実践の方策の提示**
SSDFタスク毎に、適用可能な（実践の自動化・省力化が見込める）ツール等を洗い出し、当該ツール等を活用した効率的なSSDFの導入・実践の実証を行い、ツール等の適用方法などについて整理する。

② **個別産業分野の特性に応じたSSDFの活用策の提示**
例として金融分野は、セキュリティ・バイ・デザイン、モニタリング検査、サードパーティリスク管理等を重視した対応が求められる特性があると想定。選定した分野でのSSDFの導入・実践の実証を行い、当該分野における要求事項等に対応するSSDFの活用策を整理する。

③ **SSDF達成プラクティスレベルの段階数の見直し検討（３段階 → ２段階（最小限／標準以上 等））**
現状においてはレベルを３段階としているが、レベル３の難度が高いことによりSSDF導入のハードルが上がる可能性がある。他方、特定の分野（金融分野など）においては高い達成レベルが求められる可能性もあるため、選定した複数分野でSSDFの導入・実践の実証を行う。

④ **SSDFタスクを実施しないことのリスクの明確化**
タスクを実施しないことにより生じるリスクや影響を具体化し、SSDF導入の必要性の明確化を図る。

⑤ **国内ガイドラインの不足事項への対応策の提示、各ガイドライン策定主体への働きかけ**
ソフトウェア・セキュリティに係る既存の国内ガイドラインの内容で、SSDFタスクを包含できていない部分への対応として、米NIST Cross-Reference Comparison Report（SSDF Reference）を参照することによって不足分の充足が可能か検討したうえで、当該ガイドラインの改訂が必要か等を経済産業省から各ガイドライン策定主体に検討を促す。

⑥ **自己チェックリストの検討及び案の提示**
米大統領令の改訂を踏まえ、自己適合宣言の仕組み・政府調達等での要件化等ではなく、国内事業者に自己チェックリスト（第三者による管理・運用を伴わないもの）を活用してもらう形とし、同リストの案を作成する。

議題

1. ソフトウェアの安全な利活用に関する海外の動向 【説明：三菱総合研究所】（資料４）
2. SSDFの活用促進に向けた取組の全体像【説明：経済産業省】（資料３：本資料）
3. 本年度の調査・実証の進め方 【説明：経済産業省】（資料３：本資料）
4. **本年度の調査・実証の進め方（詳細） 【説明：三菱総合研究所】（資料５）**

ご議論いただきたいこと

- 本年度の調査・実証の進め方について
  - 実証方法・進め方等について
  - ヒアリング先についてのご提案
  - 自己チェックリスト案の活用方法／プロセス案
  - 優先して取り組むべき事項（AIを活用したソフトウェア開発への対応）
  - 参照すべき情報、その他ご提案 等

- 取組の全体像について（次年度に向けた論点）
  - 効果的な普及促進策
  - システム開発等で生成AI等を活用するうえでの課題（SSDF for/by AI、SBOM for/by AI）