

「ソフトウェア管理に向けた SBOM (Software Bill of Materials) の導入に関する手引 ver2.0 (案)」に対する意見募集要領

令和 6 年 4 月 26 日
経済産業省商務情報政策局
サイバーセキュリティ課

1. 意見公募の趣旨・目的・背景

近年、産業活動のサービス化に伴い、企業において、オープンソースソフトウェア (OSS) を含むソフトウェアの利用が広がっています。例えば、産業機械や自動車等の制御においてソフトウェアの導入が進んでいます。また、IoT 機器・サービスや 5G 技術についても、汎用的な機器でハードウェア・システムを構築した上で、ソフトウェアにより多様な機能を持たせることで、様々な付加価値を創出していくことが期待されています。

このように産業に占めるソフトウェアの重要性が高まる一方で、ソフトウェアの脆弱性を突いたサイバー攻撃が企業経営に大きな影響を及ぼすなど、ソフトウェアに対するセキュリティ脅威が増大しています。このため、自社のセキュリティを強化するためにソフトウェアを適切に管理していくことが重要になりますが、ソフトウェアサプライチェーンが複雑化し、OSS の利用が一般化する中で、自社製品において利用するソフトウェアであっても、コンポーネントとしてどのようなソフトウェアが含まれているのかを把握することが困難な状況という課題があります。

このようなソフトウェアの脆弱性管理に関し、ソフトウェアの開発組織と利用組織双方の課題を解決する一手法として、「ソフトウェア部品表」とも呼ばれる SBOM (Software Bill of Materials) を用いた管理手法が注目されています。

経済産業省では、「産業サイバーセキュリティ研究会ワーキンググループ 1 (制度・技術・標準化) 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」において、有識者や様々な分野の業界団体関係者を交えながら、SBOM の利活用等について実証や議論を行い、企業が適切にソフトウェアを管理するために SBOM の導入を検討する際に活用できるよう、SBOM の基本的な情報や導入に向けた実施事項、認識しておくべきポイントを整理した「ソフトウェア管理に向けた SBOM (Software Bill of Materials) の導入に関する手引 ver1.0」を 2023 年 7 月に公表しました。

他方で、SBOM を導入した後に、SBOM をどのように活用してソフトウェアの脆弱性を効率的に管理 (ソフトウェアの脆弱性の特定、脆弱性対応の優先度付け、情報共有、脆弱性対応) 出来るかが明らかでないといった課題が存在しています。

また、ソフトウェア部品の供給者と調達者の立場によって、SBOM 作成のコストや脆弱性管理の効率化による便益に偏りが発生しないよう、SBOM 導入前に取り決めに明確にしておくことや、SBOM により特定されるソフトウェア部品の範囲や脆弱性管理の範囲などどこまで対応出来ているか違いを可視化し、分野や用途に応じて SBOM を導入するのに適切な範囲を明らかにすることも重要です。

これらの課題を対応し、産業界における SBOM の活用をさらに促すべく、同タスクフォースにおいて検討を進め、今般、「ソフトウェア管理に向けた SBOM (Software Bill of Materials) の導入に関する手引 ver2.0 (案)」を策定しました。

「ソフトウェア管理に向けた SBOM (Software Bill of Materials) の導入に関する手引 ver2.0 (案)」は、ソフトウェアを供給する企業と調達する企業の双方を想定読者としています。

2023 年7月に公表した「ソフトウェア管理に向けた SBOM の導入に関する手引 ver1.0」の内容に加えて、以下の内容を盛り込んでいます。

①脆弱性管理プロセスの具体化(第7章)

SBOM を活用することで、ソフトウェアの脆弱性管理を通じた脆弱性リスクの低減が効果として見込まれていることから、SBOM を活用するプロセスの中でも、脆弱性管理に関するフェーズが特に重要です。本章では、ソフトウェアの脆弱性を管理する一連プロセスにおいて SBOM を効果的に活用するための具体的な手順と考え方をまとめることで、SBOM 活用による効果を高めるための参考情報を提供しています。

②「SBOM 対応モデル」の追加(8.付録)

本モデルでは、SBOM 導入の効果及びコストを勘案して実際に SBOM を導入することが妥当な範囲を検討するためのフレームワークを示しています。当該フレームワークを用いることで、高度な管理を行えるソフトウェア、すなわちセキュアなソフトウェアが市場に適切に評価され、その流通が促進されることが期待できます。

③「SBOM 取引モデル」の追加(9.付録)

本モデルでは、ソフトウェア部品の受発注において、調達者と供給者の間で SBOM に関して契約に規定すべき事項(要求事項、責任、コスト負担、権利等)について参考となる例を示しています。

今回、「ソフトウェア管理に向けた SBOM (Software Bill of Materials) の導入に関する手引 ver2.0 (案)」について、広く国民の皆様から御意見を頂きたく、以下の要領で意見の募集をいたします。忌憚のない御意見を下さいますようお願い申し上げます。また、御提出いただいた御意見については、整理した上で検討の結果を公表することとしておりますが、個別の回答は致しかねますので、あらかじめご了承ください。

2. 意見公募の対象

○「ソフトウェア管理に向けた SBOM (Software Bill of Materials) の導入に関する手引 ver2.0 (案)」

3. 資料入手方法

電子政府の総合窓口 (e-Gov) における掲載

4. 意見募集期間 (意見募集開始日及び終了日)

令和6年4月26日(金)～令和6年5月27日(月)(必着)

5. 意見提出先・提出方法

電子政府の総合窓口 (e-Gov) における当該の「意見提出フォーム」に御意見等を入力し、提出してください。

なお、電子政府の総合窓口 (e-Gov) のご利用が難しい場合は、別紙の意見提出用紙に日本語で記入の上、以下いずれかの方法で送付して下さい。

(1) 郵送

意見提出用紙に御氏名、連絡先及び本件への御意見をご記入の上、下記の住所

宛にお送り下さい。

住所：〒100-8901

東京都千代田区霞が関1-3-1

経済産業省商務情報政策局サイバーセキュリティ課

パブリックコメント担当 あて

(2) F A X

意見提出用紙に御氏名、連絡先及び本件への御意見をご記入の上、下記のF A X 番号宛にお送り下さい。

F A X 番号：03-3580-6239

※ 電話での意見提出はお受けしかねますので、あらかじめ御了承下さい。

6. その他

皆様から御提出いただいた御意見につきましては、最終的な決定における参考とさせていただきます。なお、御提出いただいた御意見についての個別の回答はいたしかねますので、あらかじめ、その旨を御了承下さい。

御提出いただきました御意見については、氏名、住所、電話番号、F A X 番号及びメールアドレスを除き、すべて公開される可能性があることを、あらかじめ御承知おき下さい。ただし、御意見中に、個人に関する情報であって特定の個人を識別しうる記述がある場合及び個人・法人等の財産権等を害するおそれがあると判断される場合には、公表の際に当該箇所を伏せさせていただきます。

御意見に附記された氏名、連絡先等の個人情報につきましては、適正に管理し、御意見の内容に不明な点があった場合等の連絡・確認といった、本案に対する意見公募に関する業務にのみ利用させていただきます。

