一般社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report

Stack Overflow における SBOM 利活用に関する質問の分析

音田　涉† 神田　哲也† 眞鍋　雄貴†† 井上　克郎††† 肥後　芳樹†

† 大阪大学大学院情報科学研究科　〒565-0871 大阪府吹田市山田丘 1-5
†† 福知山公立大学情報学部情報学科　〒620-0886 京都府福知山市堀 3370
††† 南山大学理工学部ソフトウェア工学科　〒466-8673 愛知県名古屋市昭和区山里町 18
E-mail: †{wa-otoda,t-kanda,higo}@ist.osaka-u.ac.jp, ††manabe-yuki@fukuchiyama.ac.jp, †††inoue599@nanzan-u.ac.jp

あらまし　現在のソフトウェア開発では多くの外部ライブラリを活用するが，セキュリティや著作権上のリスクが伴う．この問題に対処するためにソフトウェア部品表（Software Bill of Materials，SBOM）の活用が奨励されているが，その普及は未だ不十分である．本研究では，開発者向け Q&A サイトである Stack Overflow における SBOM 利活用に関する質問を調べることで，開発者が実際に SBOM を活用する上で直面した課題について調査した．その結果，SBOM 利活用に関する質問のうち解決済みは 14.6% と極めて低い水準であること，2020 年から 2023 年にかけて着実に新規質問数が増加していること，SBOM 利用者が抱いている課題は SBOM 生成ツールに関する 3 つの課題に大別できることがわかった．

キーワード　SBOM, SPDX, CycloneDX, サプライチェーン, Stack Overflow

1. ま え が き

現在のソフトウェア開発は，実現する機能を全て自力で実装するのではなく，多くの外部ライブラリを活用することで行われる．これにより，開発費用の削減や開発期間の短縮に加え，既に洗練されているソフトウェア資源を活用することで，堅牢かつ高機能なソフトウェアを開発できる [1], [2]．一方で，外部ライブラリの利用には，セキュリティや著作権上のリスクが伴う．まず，開発しているソフトウェアが依存する外部ライブラリに脆弱性が見つかった場合，それが依存元にも波及して悪意のある利用者による攻撃の対象となるリスクがある [3]．また，開発しているソフトウェアが依存する外部ライブラリの開発者が悪意のある処理を埋め込むリスクや，外部ライブラリの開発者が悪意を持った人物による乗っ取り被害にあうリスクも存在する [4]．実際に，SolarWinds 製ソフトウェア Orion の更新データにサプライチェーン攻撃によってマルウェアが埋め込まれ，Orion を利用する多数の米国省庁や民間企業がサイバー攻撃を受ける事件が 2020 年に発生した [5]．さらに，ソフトウェアには著作権が存在し，各開発者が利用条件を定めてライセンスしているが，その条件の把握漏れにより条件に反した利用を行うことや，互いに条項が衝突するライセンスが設定されたライブラリを導入することなどにより，著作権侵害となる法的リスクも存在する [6]．これらのリスクは早期に発見し対応することが重要となるが，現在のソフトウェア開発で利用する外部ライブラリの数は，その外部ライブラリが依存する別のライブラリのような推移的な依存関係も考慮すると膨大なものとなり [7]，適切な管理は難しい．

この問題に対処するために，ソフトウェア部品表（SBOM）の活用が奨励されている．しかし，SBOM の普及は未だ不十分であることが指摘されている [8], [9]．これに対し，企業や組織に対する実態調査を行うことで原因や改善案を示した研究は存在するが，一般の開発者が実際に SBOM を活用する上で直面した課題について調査した研究は存在しない．そこで本研究では，開発者向け Q&A サイトである Stack Overflow における SBOM 利活用に関する質問を調査した．

調査 1：SBOM 利活用に関する質問の回答・解決状況
SBOM 利活用に関する質問について回答状況と解決状況を調べることで，SBOM 利用者が課題に直面した際に Stack Overflow で質問すれば解決できる状況になっているかどうかを調査する．

調査 2：SBOM 利活用に関する質問数の推移
SBOM 利用を求める米国大統領令の発令や SPDX の ISO/IEC 標準化など，SBOM を取り巻く状況は変化している．その SBOM 普及への影響を調査するため，Stack Overflow における SBOM 利活用に関する質問数の推移を調べる．

調査 3：SBOM 利用者が抱いている課題
Stack Overflow 上の SBOM 利活用に関する質問内容を調べることで，実際に SBOM を利用するソフトウェア開発者が抱いている課題を調査する．

調査 1 では，SBOM 利用者が課題に直面した際に Stack Overflow で質問することでは解決が難しい状況であることを明らかにした．調査 2 では，SBOM 利用を求める米国大統領令の発令や SPDX の ISO/IEC 標準化が行われた 2021 年以降，特に新規質問数が増加していることを明らかにした．調査 3 では，SBOM 利用者が抱いている課題は SBOM 生成ツールに関する 3 つの課題に大別できることを明らかにした．

以降，2 節では研究背景や関連研究について述べる．3 節では本研究の調査方法について述べ，4 節では得られた結果と考

察を述べる．最後に，5 節では妥当性への脅威と，6 節では本研究のまとめと今後の課題を述べる．

2. 背　　景

開発者向け Q&A サイトとして主要なものに Stack Overflow があり，SBOM を利用活用する際に課題に直面した開発者が，その解決法について質問している可能性が高い．本節では SBOM と Stack Overflow について説明し，SBOM の普及に関する既存の調査研究を紹介する．

2.1 SBOM

SBOM は，ソフトウェアの構築に用いられるライブラリなどのソフトウェア部品の正式かつ機械可読な表であり，各ソフトウェア部品のライセンス・バージョン・ベンダなどの詳細や，部品間のサプライチェーン関係の情報を含む [10], [11]．公機関も SBOM 利用を推進するなど，近年急速に注目が集まっている．米国では，Biden 政権が大統領令 Executive Order on Improving the Nation's Cybersecurity を 2021 年に発令して SBOM 利用を推進した [12]．EU でも，ENISA(注1)が IoT セキュリティにおける SBOM 利用を推奨する Guidelines for Securing the Internet of Things を公開したほか [13]，SBOM 利用を推進する Cyber Resilience Act も発効に向けた準備が進んでいる [14]．日本でも，経済産業省が「ソフトウェア管理に向けた SBOM の導入に関する手引」を公開した [15]．SBOM を表現する方法として，最も主要なものは CycloneDX と SPDX の 2 つの形式である [16]．CycloneDX はセキュリティ団体 OWASP が定める規格であり，ソフトウェア部品，外部サービス，それらの関係性を表現可能であるなど，セキュリティやサプライチェーン部品の解析を念頭に設計されている [17]．一方，SPDX は Linux Foundation を起源とする ISO/IEC 5962:2021 標準規格であり，開発フローや業務におけるコンプライアンス遵守や透明性確保を行うことを念頭に設計されている [18]．

2.2 Stack Overflow

Stack Overflow は，質問とそれに対する回答を投稿・検索できる開発者に特化した Q&A サイトであり，あるユーザの質問に不特定多数のユーザが回答する．Stack Overflow における質問の例を図 1 に示す(注2)．Stack Overflow における投稿は，タイトル，質問，複数個のタグ，そして質問に対する複数の回答で構成される．複数の回答のうち，質問の解決に最も貢献したと質問者が判断した回答 1 つについては，緑色のチェックマークで表される Accepted が付与される．ただし，どの回答でも質問が解決されなかった場合など，どの回答にも Accepted が付与されないこともある．

Stack Overflow は 2024 年 2 月現在，ユーザ数は約 2,200 万人，投稿は質問と回答を合わせて約 6,000 万件，そして 1 日に約 2,700 件の質問が投稿されており，広く普及していることがわかる [19]．新たなツールや技術の調査にも広く用いられており，新たなツールの評価にあたり Stack Overflow などの開発者

(注1)：The European Union Agency for Cybersecurity
(注2)：https://stackoverflow.com/questions/69121175

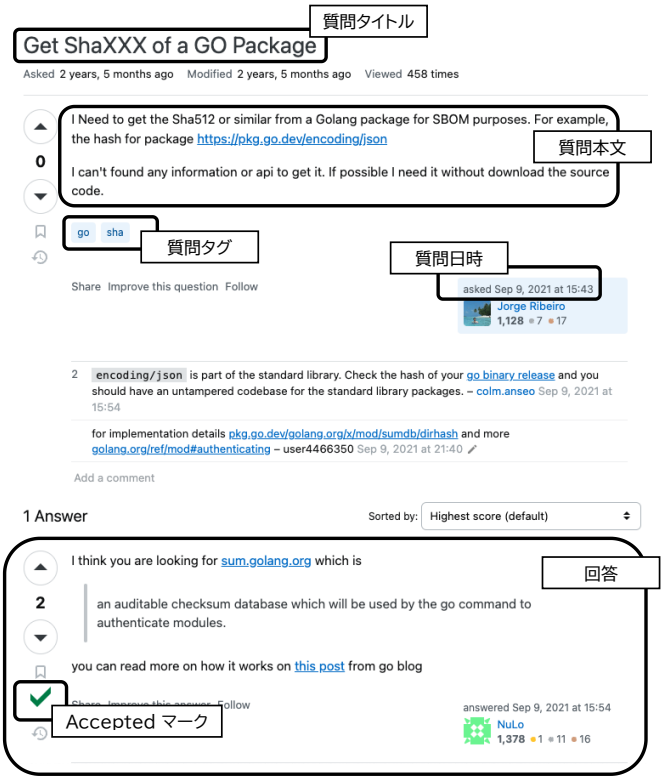

図 1　Stack Overflow における質問の例

コミュニティを利用すると答えた開発者は 64.11% と，無料トライアルを開始する，知り合いの開発者に質問するに続く第 3 位である [20]．

2.3 既存研究

Linux Foundation により，2022 年に SBOM 準備度調査が実施された [11]．これは多種多様な業種・規模の 412 の組織を対象としたものであり，76% の組織が SBOM 導入に取り組んでいるものの，40% の組織が業界の SBOM 導入への積極性，39% が SBOM に含めるべき情報に関する業界合意の有無，37% が SBOM によって顧客にもたらされる価値の不明瞭さについて不安を抱いていることを明らかにした．また，Xia らも SBOM の普及状況や課題についてのインタビュー調査を実施した [8]．これは SBOM を利用する開発者を対象としたものであり，SBOM 生成のインセンティブ，SBOM に含めるべき情報の合意，SBOM の情報を部分的に開示する仕組み，SBOM の内容検証，成熟した SBOM ツール，SBOM の認知度向上などの重要性を指摘した．さらに，Stalnaker らはステークホルダーが SBOM の作成時や使用時に直面した課題と，課題への対処法を調査した [21]．これは SBOM コミュニティと採用者，主要 OSS の貢献者，サイバーフィジカルシステム（CPS）の開発者及び研究者，人工知能・機械学習の開発者及び研究者，法務者を対象としたものであり，複雑な SBOM 仕様の目的別整理，ツールとビルドシステムの SBOM サポート，SBOM の内容検証，SBOM 導入のインセンティブが重要だと指摘した．

これらの調査は業界における SBOM の現状と今後取り組むべき課題に関して洞察を与えるものであるが，企業や組織に所属しない一般のソフトウェア開発者は対象としていない．こ

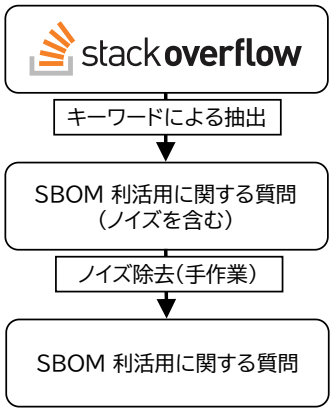

図 2　調査の流れ

れに対し，Nocera らは個人利用・業務利用共に最も主要なソフトウェア開発プラットフォームである GitHub 上の OSS に対して SBOM の利用状況の調査を行った [9]．その結果として，OSS があまり SBOM を導入していないこと，その中でもコード変更の都度 SBOM を更新し同梱するなどの NTIA(注3) が定めるガイドライン [10] を満たしているものは少ないこと，CI/CD やビルドに統合できる SBOM 生成ツールの拡充が重要であることを指摘した．しかし，これは定量的調査であり，具体的にソフトウェア開発者が直面している課題を明らかにしたものではない．

3. 調　　査

3.1 調査データの抽出

本研究では，SBOM フォーマットとして CycloneDX と SPDX を対象とし，Stack Overflow における SBOM 利活用に関する質問について調査を行った．

調査の実施にあたり，図 2 の処理を行う．まず，検索キーワードとして「SBOM」，「CycloneDX」，「SPDX」を選出した．大文字小文字は区別せず，タイトルまたは本文にこれらのキーワードのうち少なくとも 1 つが含まれる質問を抽出する．Stack Overflow には質問内容に応じてタグを設定する機能があるが，調査時点で SBOM 関連のタグはほとんど利用されていないため使用しない．その後，利用しているフレームワークが SBOM にまつわる文字列を出力した，ソースコード中に SBOM に関する文字列が含まれていた，などといった SBOM 利活用に関する質問ではないもの（以下ノイズと呼ぶ）を取り除く．

キーワード「SBOM」と「CycloneDX」については Stack Overflow のサイト上の検索ボックスから，それぞれ `SBOM is:question`，`CycloneDX is:question` と入力して検索し，得られたものからノイズを手作業で取り除く．大文字小文字は区別されず，`is:question` によって質問のみが検索結果に表示される．ただし，次のキーワード「SPDX」で用いるデータベースが 2023 年 9 月版であるため，一貫性を保つために 2023 年 8 月中までの質問のみを対象とする．

キーワード「SPDX」については Stack Exchange Data Dump 2023-09-12(注4) を利用し，後述するノイズパターンを機械的に取り除いたのちに残ったノイズを手作業で取り除く．ここで，キーワード「SBOM」と「CycloneDX」については Web サイトから直接検索したのに対し，キーワード「SPDX」ではデータダンプを用いた理由は，検索時にマッチした質問件数が前者はそれぞれ 57 件，31 件だったのに対し，後者は Stack Overflow の検索機能の上限である 500 件を超えたためである(注5)．キーワード「SPDX」における手動でのノイズ除去は，データダンプから機械的にノイズパターンを取り除いた後に得られる投稿について，質問ページを閲覧して行う．

表 1 に，除外するノイズパターンとその集計結果を示す（重複を含む）．ノイズパターンは，ノイズを手作業で除外する過程で SBOM の利活用に無関係な投稿に頻出する文字列を抽出し，それが SPDX 形式の SBOM に現れるパターンでないことを確認した上で選定した．以下，各ノイズパターンの選定理由を説明する．`SPDX-License-Identifier` は，プログラムコード冒頭でライセンスを宣言する際に使用する統一的な記法であり，この宣言を含むプログラムコードを掲載する質問がマッチしていた．これは SPDX 規格の一部として Linux Foundation により定められているものである [22] が，これ自身は SBOM ではなく，また SPDX 形式の SBOM に現れることもないため除外した．同様に，`License should be a valid SPDX license expression` は，JavaScript 向けのパッケージ管理システム Yarn が，パッケージに設定されたライセンス表記が誤っている場合に出力する警告メッセージであるため除外した．`spdy` は，プログラム中で x 軸の速度を表す変数名として `spdx`（大文字小文字の組み合わせが異なるものも存在）を用いているケースがあり，これらのケースでは概ね y 軸の速度を表す `spdy` を伴うことから除外した．`spdx-correct`, `spdx-expression-parse`, `spdx-exceptions`, `spdx-license-ids` はいずれもパッケージ管理システム NPM 上のパッケージ名であるが，NPM のエラーに関する質問で，対象のプロジェクトの依存関係としてこれらのパッケージが含まれることで，ログ中にこれらのパッケージ名が現れるケースがほとんどだったため取り除いた．

この処理の結果，キーワード「SBOM」では 27 件，「CycloneDX」では 28 件，「SPDX」では 6 件の質問が抽出された．

表 1　キーワード「SPDX」におけるノイズパターン

ノイズパターン	件数
`SPDX-License-Identifier`	1229
`License should be a valid SPDX license expression`	30
`spdy`	51
`spdx-correct`, `spdx-expression-parse`, `spdx-exceptions`, `spdx-license-ids`	62

(注3)：National Telecommunications and Information Administration

(注4)：`https://archive.org/details/stackexchange_20230912`

(注5)：Web サイト上の検索ボックスにもキーワード除外機能が存在するが，Stack Overflow 上では投稿が単語ごとにインデックスされているため，複数の単語で構成されるノイズパターン文字列を除外する検索が正しく動作しなかった．

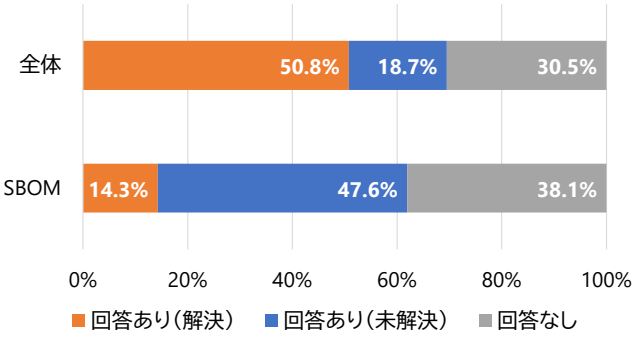

図 3　質問の回答・解決状況

また，全体としては重複があるため 42 件となった．

3.2　調 査 手 順

以上の準備の下で，各調査を実施する．

調査 1：得られた質問について，回答の有無や解決状況を調べる．Accepted 回答が存在する質問を解決，存在しない質問を未解決とみなす．

調査 2：得られた質問について，投稿日時を元に各年ごとに分類する．投稿日時は最終更新ではなく，Stack Overflow のサイト上で「asked Mar 10, 2021 at 10:35」のように記載される初出の日時を使用する．

調査 3：各質問の内容から技術課題を読み取り，頻繁に質問されている内容や未解決と思われる技術課題を筆頭著者の主観により抽出する．

4.　調査結果と考察

4.1　調査 1：SBOM 利活用に関する質問の回答・解決状況

「回答あり（解決）」,「回答あり（未解決）」,「回答なし」に分類した結果と，2024 年 2 月 1 日現在の Stack Overflow 全体の状況 [23] を図 3 に示す．SBOM 利活用に関する質問全 42 件中，回答あり（解決）は 6 件（14.3%），回答あり（未解決）は 20 件（47.6%），回答なしは 16 件（38.1%）であった．

Stack Overflow 全体における回答なしの質問の割合が 30.5% であることを考えると，SBOM 利活用に関する質問の回答状況は概ね平均的と言える．一方，Stack Oveflow 全体における解決済み質問の割合が 50.8% であることを考えると，SBOM 利活用に関する質問の解決状況は極めて低い水準であり，SBOM 利用者が課題に直面した際に Stack Overflow で質問することでは解決が難しい状況だと言える．解決済みの質問が少ない要因として，4.3.3 節も考慮すると，SBOM 利活用に関する知見が不十分で質問に回答できるソフトウェア開発者が不足していることや，SBOM 利活用の技術が未熟で質問時点では技術的に解決不可能な事項が多いことが考えられる．

4.2　調査 2：SBOM 利活用に関する質問数の推移

新規質問数の 2019 年からの 5 年間の各年ごとの推移を図 4 に示す．ただし，2023 年は 9 月時点の件数である．2018 年以前は，3. 節の手順で抽出された質問件数が 2012 年のみ 1 件，それ以外は 0 件であった．

Stack Overflow には 2024 年 2 月現在，全体で約 2400 万件の質問が存在し，1 日に約 2,700 件の質問が投稿されている [19] ことを考えると，本調査で抽出された SBOM 利活用に関する質問は 4 年間を通して少数である．しかし，2020 年から 2023 年にかけて着実に新規質問数が増加しており，特に SBOM 利用を求める米国大統領令の発令や SPDX の ISO/IEC 標準化が行われた 2021 年以降に，因果関係は断定できないがその傾向が加速していることがわかる．

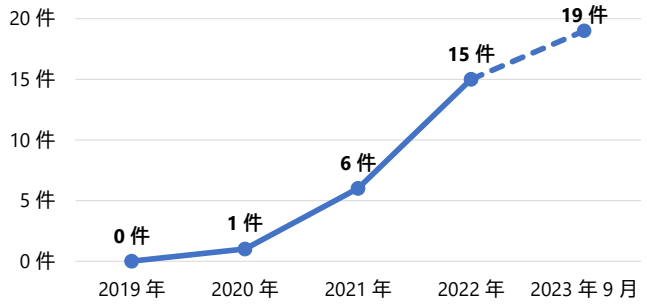

図 4　SBOM 利活用に関する新規質問数の推移

4.3　調査 3：SBOM 利用者が抱いている課題

大きく以下の課題が挙げられることがわかった．

（1）　SBOM 生成ツールのユースケースの網羅性に不足がある

（2）　各種要件を満たす SBOM を生成できない

（3）　SBOM 生成ツールに不具合がある，または利用方法が不明瞭

以降，それぞれについて代表的なものを抜粋して紹介する．

4.3.1　SBOM 生成ツールのユースケースの網羅性に不足がある

2022 年 3 月

How do I generate a Cyclonedx bom for a Java project built with Ant?(注6)

I'm already generating boms and using them with Dependency Track for some projects built with Gradle. There's a CycloneDx Gradle plugin that works well for that. However I'm also working with many older Java projects that are built with Ant. I've not been able to find an Ant tool to generate the boms anywhere. Is there one out there? If not, what's the best way to generate the bom files?. . .

これは，Gradle を用いて開発されている Java プロジェクトに対しては SBOM 生成経験があるソフトウェア開発者が，Apache Ant を用いて開発されている Java プロジェクトに対する SBOM 生成ツールを見つけられず，生成方法を求めている質問である．CycloneDX Core (Java)(注7) を使えば生成できる可能性があると指摘している回答があるが Accepted ではない．Gradle に対して Apache Ant は旧式のプロジェクト管理システムであるために SBOM 生成ツールが開発されていないと考えられる．

(注6)：https://stackoverflow.com/questions/71605182
(注7)：https://github.com/CycloneDX/cyclonedx-core-java

2022 年 9 月

Is there any tool through which we can generate SBOM report (SPDX / CycloneDX) for Windows programs?(注8)

. . . There are many tools available which can scan Linux OS packages and application packages (e.g java, maven, .net) like Trivy, Syft, whitesource but it looks like there is no tool available which can generate SBOM report for the applications installed on Microsoft Windows.. . .

これは，Linux においては Syft などのツールを用いればインストールされたソフトウェアの SBOM を生成できるが，Windows ではそれを行えるツールが見つからないという質問である．こちらも回答があるが Accepted ではない．Linux では APT や Yum といったパッケージマネージャを使ってソフトウェアをインストールすることが多い一方，Windows ではパッケージマネージャを使わずに直接インストールすることが多い．そのため，Windows では集権的にソフトウェアのメタ情報が管理されておらず，個別のソフトウェアがシステムに登録する情報しか取得できない背景から，Windows に対応する SBOM 生成ツールの開発が追い付いていないと考えられる．

4.3.2 各種要件を満たす SBOM を生成できない

2023 年 4 月

NTIA minimum SBOM requirement tool(注9)

I am trying to generate SBOM for Java, Python, ios (Swift) and Android (kotlin) project. I need to follow the NTIA guidelines for minimum element for SBOM (`https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf`). These elements are Supplier Name, Component Name, Version of the component, Other identifier, dependency relationship, Author of SBOM data and timestamp. I tried command line SNYK and SYFT to generate SBOM for my projects Java and Python projects in SPDX format. Neither of the tools generates Supplier name. Syft did not generate the SBOM for my ios project. Still to perform SNYK test for ios project. Have anyone used some other tools to generate SBOM with minimum NTIA required fields. Is there any tool to generate report in word or pdf format based on the generated json?

これは，開発者が Java と Python について SBOM 生成を試みたものの，NTIA が発行するガイドライン [10] の要件を満たす SBOM を生成するツールを見つけられず，そのようなツールを求めている質問である．このガイドラインは 2021 年 7 月に，SBOM 利用を求める大統領令の発令に伴い発行されたものであるが，全てのツールがそれに追従しきれていないか，ツールの実装においてガイドラインに定められる情報の入手が困難などの課題があることを表していると考えられる．

2023 年 8 月

How to include Open Source license in GitHub SBOM export?(注10)

Is there a way to include the Open Source license in the GitHub SBOM export? If not is there a way to easily generate a list of dependencies that includes the name, version, and open source license for a GitHub repo? I tried the Export SBOM under dependencies but this does not seem to include the Open Source license for the dependencies.

GitHub には，GitHub がリポジトリ内に置かれたパッケージマネージャのファイルなどの各種メタデータを用いて自動生成した SPDX 形式の SBOM を，Dependency graph からダウンロードできる機能が存在する．この質問では，依存するパッケージに関するライセンス情報が含まれていないため，これを含める方法を求めている．コンプライアンス管理などの目的でライセンス情報が求められる状況において，GitHub の SBOM 生成機能では不足があることを表している質問だと考えられる．

4.3.3 SBOM 生成ツールに不具合がある，または利用方法が不明瞭

2023 年 6 月

How to create a BOM file in a Flutter project(注11)

I'm trying to create a BOM file for the Android portion of a Flutter project for security scanning. I added org.cyclonedx.bom (a gradle plugin) to gradle and I'm running the cyclonedxBom gradle task, but I'm getting an error:. . .

これは，Flutter を用いるソフトウェア開発者が CycloneDX 形式の SBOM 生成を試みたものの，エラーが出て生成できなかったという質問である．この他にも，エラーの解決法や，SBOM 生成ツールの使い方に関する質問が多く存在した．これらの質問は，SBOM 生成ツールが比較的若いソフトウェアであることから十分に成熟しておらず，不具合や機能不足によって正しく SBOM 生成ができないケースが存在することや，SBOM 生成に関するドキュメントや知見が十分に蓄積されておらず，ソフトウェア開発者が SBOM 生成ツールの基本的な利用方法を理解できていないことを示唆していると考えられる．

4.3.4 全体の考察

抜本的に新しいアプローチのツール・システムを必要とする課題に関する質問はわずかであり，既存ツールの使い方や不具合，既存ツールでは実現できない些細な機能に関する質問が多かった．ここから，多くの一般の開発者は，既存ツールの扱い方に関する知見の充実と，既存ツールの洗練や機能拡張を求めていると考えられる．

5. 妥当性への脅威

5.1 ノイズの除外方法

本調査では，キーワード「SPDX」を含む質問の調査において表 1 のキーワードを除外した．しかし，これにより本来除外

(注8)：https://stackoverflow.com/questions/73648096
(注9)：https://stackoverflow.com/questions/76103711
(注10)：https://stackoverflow.com/questions/76962834
(注11)：https://stackoverflow.com/questions/76515339

されるべきではない，ノイズに当たらない SBOM 利活用に関する質問が除外された可能性がある．ただし，除外キーワードの選定にあたっては，実際にそのキーワードを含む投稿を複数抽出して調査することで，該当の除外キーワードを含む投稿がノイズである可能性が高いことを確認しているため，これによる妥当性への脅威は小さいと考えられる．

5.2 調 査 数

本調査において，条件を満たすものとして抽出された質問数は全体で 42 件とごく少数であった．SBOM が未だ十分に普及していないことが原因と考えられるが，調査結果の正確性に悪影響を与えている可能性がある．一方，Stack Overflow 以外にも Quora などの一般の Q&A サイトが存在するが，簡単に調べた範囲では SBOM に携わる開発者や管理者がそれらを利用して問題解決を活発に行っている様子はみられなかった．

6. まとめと今後の課題

本研究では，開発者向け Q&A サイト Stack Overflow に投稿された，SBOM 利活用に関する質問内容の調査を行った．具体的には，SBOM 利活用に関する質問の回答・解決状況（調査 1），SBOM 利活用に関する質問数の推移（調査 2），SBOM 利用者が抱いている課題（調査 3）の調査を行った．

調査 1 では，解決している質問は 14.3% と Stack Overflow 全体における 50.8% に対して極めて低い水準であり，SBOM 利用者が課題に直面した際に Stack Overflow で質問することでは解決が難しい状況であることがわかった．調査 2 では，SBOM 利用を求める大統領令や SPDX の ISO/IEC 標準化などがなされた 2021 年以降に新規質問数の増加が加速していることがわかった．調査 3 では，SBOM 利用者が抱いている課題が「SBOM 生成ツールのユースケースの網羅性に不足がある」，「各種要件を満たす SBOM を生成できない」，「SBOM 生成ツールに不具合がある，または利用方法が不明瞭である」の 3 つであることがわかった．

今回の結果から，SBOM に対する潜在的な疑問質問は多く存在すると思われるが，Stack Overflow への投稿数は少ない．Stack Overflow が投稿先として適切でないと思われているためか，SBOM が十分に普及していないためかなど，今後の理由の分析が必要である．そのために，質問数が増加傾向にある Stack Overflow の調査を継続するとともに，Reddit のような Stack Overflow 以外の Web サイトでも調査を行うことで，SBOM 利活用の最新のトレンドを追跡することが，今後の課題として考えられる．

謝辞 本研究は，JSPS 科研費（JP23H03375，JP21K02862，JP19K20239，JP22K11985），2023 年度南山大学パッヘ研究奨励金 I-A-2 の助成を得て行われた．

文 献

[1] O.P.N. Slyngstad, A. Gupta, R. Conradi, P. Mohagheghi, H. Rønneberg, and E. Landre, “An Empirical Study of Developers Views on Software Reuse in Statoil ASA,” Proc. ISESE2006, pp.242–251, 2006.

[2] W.C. Lim, Managing software reuse : a comprehensive guide to strategically reengineering the organization for reusable components, Prentice Hall, c1998. https://ci.nii.ac.jp/ncid/BA49519010

[3] Y. Wang, B. Chen, K. Huang, B. Shi, C. Xu, X. Peng, Y. Wu, and Y. Liu, “An Empirical Study of Usages, Updates and Risks of Third-Party Libraries in Java Projects,” Proc. ICSME2020, pp.35–45, 2020.

[4] M. Ohm, H. Plate, A. Sykosch, and M. Meier, “Backstabber’s Knife Collection: A Review of Open Source Software Supply Chain Attacks,” Proc. DIMVA2020, pp.23–43, 2020.

[5] E.D. Wolff, K.M. Growley, M.O. Lerner, M.B. Welling, M.G. Gruden, and J. Canter, “Navigating the solarwinds supply chain attack,” The Procurement Lawyer, vol.56, no.2, pp.3–10,28, Spring 2021.

[6] 経済産業省 商務情報政策局 サイバーセキュリティ課，“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,” https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/002_03_00.pdf，2019．

[7] R. Kikas, G. Gousios, M. Dumas, and D. Pfahl, “Structure and Evolution of Package Dependency Networks,” Proc. MSR2017, pp.102–112, 2017.

[8] B. Xia, T. Bi, Z. Xing, Q. Lu, and L. Zhu, “An Empirical Study on Software Bill of Materials: Where We Stand and the Road Ahead,” Proc. ICSE2023, pp.2630–2642, 2023.

[9] S. Nocera, S. Romano, M. Penta, R. Francese, and G. Scanniello, “Software Bill of Materials Adoption: A Mining Study from GitHub,” Proc. ICSME2023, pp.39–49, Oct. 2023.

[10] The United States Department of Commerce, “The Minimum Elements For a Software Bill of Materials (SBOM),” https://www.ntia.gov/report/2021/minimum-elements-software-bill-materials-sbom, 2021.

[11] S. Hendrick and J. Zemlin, “The State of Software Bill of Materials (SBOM) and Cybersecurity Readiness,” https://www.linuxfoundation.org/research/the-state-of-software-bill-of-materials-sbom-and-cybersecurity-readiness, 2022.

[12] J. Biden, “Executive Order on Improving the Nation’s Cybersecurity | The White House,” https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/, 2021.

[13] The European Union Agency for Cybersecurity, “Guidelines for Securing the Internet of Things － ENISA,” https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things, 2020.

[14] European Commission, “Cyber Resilience Act | Shaping Europe’s digital future,” https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454, 2022.

[15] 経済産業省 商務情報政策局 サイバーセキュリティ課，“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 Ver. 1.0,” https://www.meti.go.jp/press/2023/07/20230728004/20230728004-1-2.pdf，2023．

[16] B. Bensing, “History of the Software Bill of Material (SBOM) - Bill Bensing,” https://billbensing.com/software-supply-chain/history-software-bill-of-material-sbom/, 2022.

[17] OWASP Foundation, “CycloneDX - Software Bill of Materials (SBOM),” https://cyclonedx.org/capabilities/sbom/.

[18] The Linux Foundation, “Overview － SPDX,” https://spdx.dev/about/overview/.

[19] Stack Exchange Inc., “All Sites - Stack Exchange,” https://stackexchange.com/sites?view=list.

[20] Stack Overflow, “Stack Overflow Developer Survey 2023,” https://survey.stackoverflow.co/2023/, 2023.

[21] T. Stalnaker, N. Wintersgill, O. Chaparro, M.D. Penta, D.M. German, and D. Poshyvanyk, “BOMs Away! Inside the Minds of Stakeholders: A Comprehensive Study of Bills of Materials for Software Systems,” 2024.

[22] Linux Foundation and its Contributors, “Annex E: Using SPDX short identifiers in Source Files - specification v2.3.0,” https://spdx.github.io/spdx-spec/v2.3/using-SPDX-short-identifiers-in-source-files/, 2022.

[23] Stack Overflow, “Usage of /info [GET] - Stack Exchange API,” https://api.stackexchange.com/docs/info#filter=default&site=stackoverflow&run=true.