

2023年4月7日
ギットハブ・ジャパン合同会社

GitHub、クラウドリポジトリ向けの 新しい SBOM 生成ツールの提供を開始

オープンソースプロジェクトおよびビジネスユースを含む、ソフトウェアの開発プラットフォームを提供する GitHub, Inc.（本社：米国サンフランシスコ）は、2023年3月28日(米国時間)に開発者とコンプライアンスチームの方々を対象に、クラウドリポジトリ向けの新しい SBOM 生成ツールの提供を開始しました。



サイバーセキュリティの強化に関する [大統領令第 14028 号](#) という先例に倣い、セキュリティやコンプライアンスチームからのソフトウェア部品表 (SBOM) の要求が増加しています。この目的は、ソフトウェアプロジェクトのオープンソースコンポーネントを特定し、新たな脅威に対するその脆弱性を評価したり、ライセンスポリシーとの整合性を確認することであり、そのため SBOM を簡単に生成し、共有することが求められています。

GitHub は、新たに導入する Export SBOM 機能において、GitHub のクラウドリポジトリに対する読み取りアクセス権のあるユーザーなら誰でも、クリック 1 回で [NTIA](#) 準拠の SBOM を生成できることを発表しました。作成された JSON ファイルは、バージョンやライセンスなどプロジェクトの依存関係とメタデータを業界標準の SPDX 形式で保存するため、セキュリティおよびコンプライアンスのワークフローやツールで利用したり、Microsoft Excel でレビューするこ

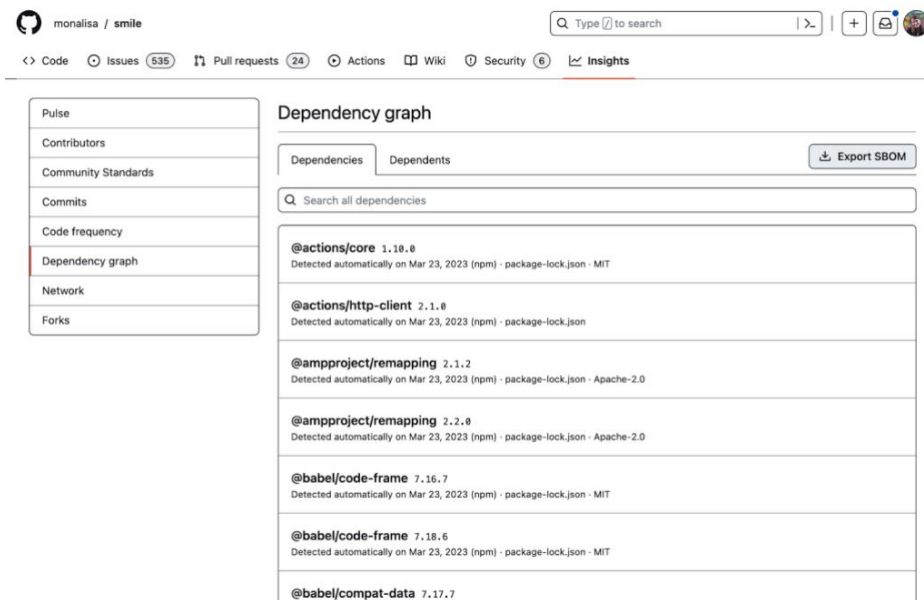
とが可能です(JSON から CSV へのコンバーターを使うと Google Sheets との互換性も確保できます)。

本セルフサービスの新機能を利用することで、オンデマンドで簡単に SBOM を生成できるほか、開発者が開発ワークフローの通常のステップに SBOM 生成を組み込むことも可能です。すでにプロジェクトの SBOM がある場合は、[依存関係グラフにアップロード](#)することで既知の脆弱性があるすべての依存関係に関して Dependabot アラートを受信できます。また、[GitHub の SBOM gh CLI 拡張機能](#)を使用して、リポジトリの依存グラフから SBOM をプログラムで生成できるほか、[GitHub Action](#)により、ビルド時に SBOM を生成することもできます。今後、依存関係グラフから SBOM を生成する REST API も近日中に提供予定です。

セルフサービスの SBOM は、GitHub のサプライチェーンセキュリティソリューションの一環として、GitHub のすべてのクラウドリポジトリで無料で利用できます。

変更点

SBOM を生成するには、リポジトリの依存グラフにある新しい[Export SBOM] ボタンをクリックしてください。



The screenshot shows the GitHub web interface for a repository named 'monalisa / smile'. The 'Dependency graph' section is active, displaying a list of dependencies. A search bar is present above the list. The dependencies listed are:

Dependency	Version	Source
@actions/core	1.10.0	Detected automatically on Mar 23, 2023 (npm) · package-lock.json · MIT
@actions/http-client	2.1.0	Detected automatically on Mar 23, 2023 (npm) · package-lock.json
@ampproject/remapping	2.1.2	Detected automatically on Mar 23, 2023 (npm) · package-lock.json · Apache-2.0
@ampproject/remapping	2.2.0	Detected automatically on Mar 23, 2023 (npm) · package-lock.json · Apache-2.0
@babel/code-frame	7.16.7	Detected automatically on Mar 23, 2023 (npm) · package-lock.json · MIT
@babel/code-frame	7.18.6	Detected automatically on Mar 23, 2023 (npm) · package-lock.json · MIT
@babel/compat-data	7.17.7	

これにより、機械可読な JSON ファイルが SPDX 形式で作成されます。

```
1 {
2   "SPDXID": "SPDXRef-DOCUMENT",
3   "spdxVersion": "SPDX-2.3",
4   "creationInfo": {
5     "created": "2023-03-21T22:39:26Z",
6     "creators": [
7       "Tool: GitHub.com-Dependency-Graph"
8     ]
9   },
10  "name": "com.github.npm/cli",
11  "dataLicense": "CC0-1.0",
12  "documentDescribes": [
13    "com.github.npm/cli"
14  ],
15  "documentNamespace": "https://github.com/npm/cli/dependency_graph/sbom-5a0298699b3caf5b",
16  "packages": [
17    {
18      "SPDXID": "SPDXRef-npm-@babel/helper-function-name-7.16.7",
19      "name": "npm@babel/helper-function-name",
20      "versionInfo": "7.16.7",
21      "downloadLocation": "NOASSERTION",
22      "filesAnalyzed": false,
23      "licenseConcluded": "MIT",
24      "licenseDeclared": "NOASSERTION",
25      "supplier": "NOASSERTION",
26      "externalRefs": [
27        {
28          "referenceCategory": "PACKAGE-MANAGER",
29          "referenceLocator": "pkg:npm/%40babel/helper-function-name@7.16.7",
30          "referenceType": "purl"
31        }
32      ]
33    },
34    {
35      "SPDXID": "SPDXRef-npm-@babel/helper-function-name-7.21.0",
36      "name": "npm@babel/helper-function-name",
37      "versionInfo": "7.21.0",
38      "downloadLocation": "NOASSERTION",
39      "filesAnalyzed": false,
40      "licenseConcluded": "MIT",
41      "licenseDeclared": "NOASSERTION",
42      "supplier": "NOASSERTION",
43      "externalRefs": [
44        {
45          "referenceCategory": "PACKAGE-MANAGER",
46          "referenceLocator": "pkg:npm/%40babel/helper-function-name@7.21.0",
```

SBOMの詳細について

- [SBOM ドキュメント](#)
- [Dependency Submission API](#)
- [GitHub SBOM コマンドラインインターフェイス\(CLI\)拡張機能](#)
- [Microsoft SBOM ツール](#)

GitHub Blog

英語：<https://github.blog/2023-03-28-introducing-self-service-sboms/>

日本語：<https://github.blog/jp/2023-04-06-introducing-self-service-sboms/>

GitHub に関する情報は、こちらからもご覧いただけます。

Blog：（英語）<https://github.blog> （日本語）<https://github.blog/jp>

Twitter：（英語）@github(<https://twitter.com/github>)

（日本語）@GitHubJapan(<https://twitter.com/githubjapan>)

【GitHub について】<https://github.co.jp>

GitHub は、すべての開発者のためのグローバルホームとして、安全なソフトウェアを構築、拡張、提供するための統合された開発者プラットフォームです。フォーチュン 100 社に採択された企業のうち 90 社に所属する開発者を含む 1 億人以上が GitHub を利用し、3 億 3 千万以上のリポジトリで素晴らしいものを共に創造しています。GitHub のすべてのコラボレーション機能によって、個人やチームがより迅速に、より高品質なコードを書くことがかつてないほど容易になっています。

【製品／サービスに関するお問い合わせ先】

ギットハブ・ジャパン営業およびサポート窓口

Email: jp-sales@github.com