

OSS紹介: SPDX用拡張機能 on VSCode

Editor for SBOM

2023/02/09

株式会社日立ソリューションズ
ITプラットフォーム事業部 デジタルシフト開発支援本部
プロセス改善ソリューション部 OSS管理ソリューショングループ

明石 知泰

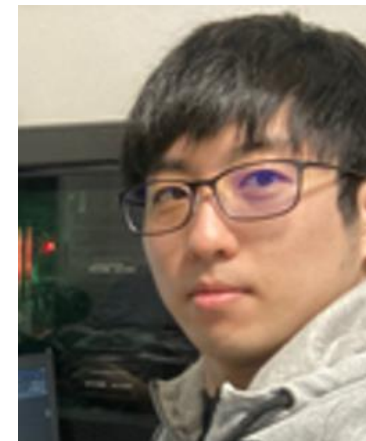
Contents

1. 自己紹介
2. デモ
3. 機能説明
4. 開発・OSS化経緯
5. おわりに

1. 自己紹介

明石 知泰

- 日立ソリューションズ所属
- 2020年に新卒入社後、現職
- メイン業務は製品開発
- 今日紹介するOSSを作った人



明石 知泰

- 2021年Qiitaアドベントカレンダーイベントで、OpenChainのカレンダーに2つ記事↓を入れてもらいました。

SPDX Documentを理解する

2021-12-01 2021-12-01

コラム SBOM SPDX



毎々お世話になっております、株式会社日立ソリューションズの明石と申します。本日は今年からSBOMフォーマットの国際標準として認定された、SPDXに準拠して作成されたSBOM、SPDX Documentについてご紹介したいと思います。

オープンソース管理ソリューション
導入から運用までOSS管理をワンストップで実現

タグ一覧

コラム パリズオン お知らせ

ライセンス セキュリティ OpenChain

SBOM SPOX OSPO ツール

WhiteSource FOSSA

新着記事

- 2022/11/2
日立建機様のOSSガイドライン策定支援に関する事例が公開されました
- 2022/11/1
SW360で使うデータの解説
- 2022/9/30
SBOMに関する質問と回答まとめ (オープンソースソフトウェアセミ)

<https://www.hitachi-solutions.co.jp/oms/sp/blog/2021120101/>

SPDX-LiteでSBOMを作ってみよう

2021-12-01 2021-12-01

パリズオン SBOM SPOX



毎々お世話になっております、株式会社日立ソリューションズの明石と申します。本日はSPDX-LiteでSBOMを作成する手順についてご紹介したいと思います。

オープンソース管理ソリューション
導入から運用までOSS管理をワンストップで実現

タグ一覧

コラム パリズオン お知らせ

ライセンス セキュリティ OpenChain

SBOM SPOX OSPO ツール

WhiteSource FOSSA

新着記事

- 2022/11/2
日立建機様のOSSガイドライン策定支援に関する事例が公開されました
- 2022/11/1
SW360で使うデータの解説
- 2022/9/30
SBOMに関する質問と回答まとめ

<https://www.hitachi-solutions.co.jp/oms/sp/blog/2021120102/>



2. デモ

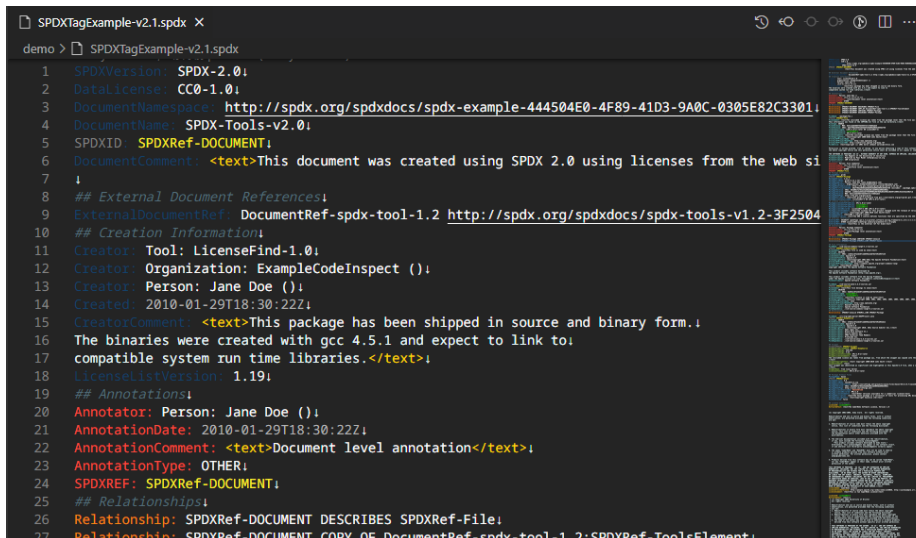
百聞は一見に如かず。

デモは以上です。

3. 機能説明

Editor for SBOM

- 要はプログラミング言語支援機能のSPDX Specification(v2.2)、tag:value(.spdx)形式版
- SBOMファイルを見る時、編集する時に使う
- Visual Studio Code専用
- MIT License

A screenshot of the Visual Studio Code editor interface. The main window displays an SPDX file named 'SPDXTagExample-v2.1.spdx'. The file content is a text-based representation of an SBOM, following the SPDX 2.0 specification. It includes fields for version, license, document namespace, name, ID, and creation information. The text is color-coded: blue for comments, green for keywords, and black for values. The editor's interface includes a sidebar on the left with a file explorer, a top toolbar with standard editing icons, and a right sidebar showing a search or source control panel. The status bar at the bottom indicates the current file is 'SPDXTagExample-v2.1.spdx'.

Syntax highlighting

- 構文、構造の色付け

- セクション

- コメント

- 特定文字列

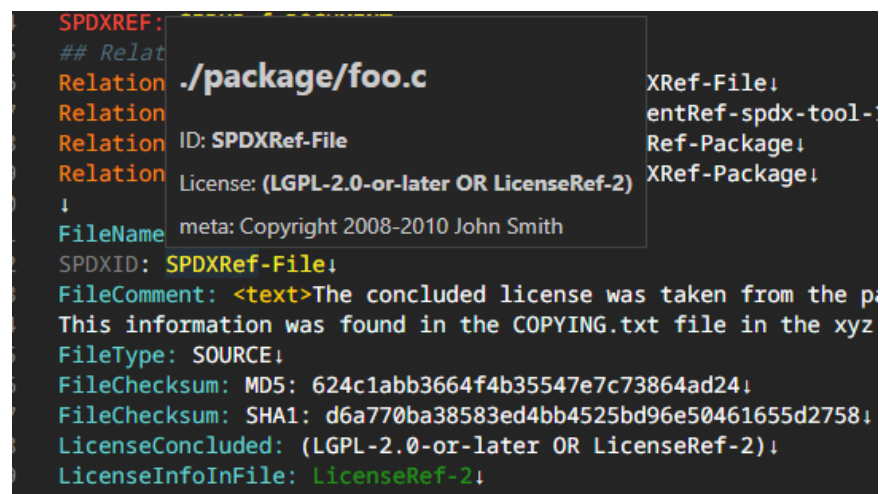
- Identifier(SPDXRef-〇〇、LicenseRef-〇〇)

- テキストタグ(<text>、</text>)

```
5 PackageLicenseConcluded: (LicenseRef-3 OR LGPL-2.0-or-later)!\n6 ## License information from files!\n7 PackageLicenseInfoFromFiles: GPL-2.0-or-later!\n8 PackageLicenseInfoFromFiles: LicenseRef-1!\n9 PackageLicenseInfoFromFiles: LicenseRef-2!\n10 PackageLicenseDeclared: (LicenseRef-3 AND LGPL-2.0-or-later)!\n11 PackageLicenseComments: <text>The license for this project changed with t\n12 PackageCopyrightText: <text>Copyright 2008-2010 John Smith</text>!\n13 PackageSummary: <text>GNU C library.</text>!\n14 PackageDescription: <text>The GNU C Library defines functions that are sp\n15 ## External references!\n16 ExternalRef: SECURITY cpe23Type cpe:2.3:a:pivotal_software:spring_framework\n17 ExternalRef: OTHER LocationRef-acmeforge acmecorp/acmenator/4.1.3-alpha!\n18 ExternalRefComment: <text>This is the external ref for Acme</text>!\n19 ## Annotations!\n20 Annotator: Person: Package Commenter!\n21 AnnotationDate: 2011-01-29T18:30:22Z!\n22 AnnotationComment: <text>Package level annotation</text>!\n23 AnnotationType: OTHER!\n24 SPDXREF: SPDXRef-Package!\n25 ## Relationship
```

Hover Information

- ファイル内識別子が示す定義情報の表示
 - SPDX ID(SPDXRef-〇〇)
 - License ID(LicenseRef-〇〇)



The screenshot shows a code editor with a dark theme. A line of code is highlighted, and a tooltip is displayed over it. The code line is: `SPDXREF: ./package/foo.c`. The tooltip contains the following information:
- **Relation**: `SPDXRef-File`
- **License**: `(LGPL-2.0-or-later OR LicenseRef-2)`
- **FileName**: `meta: Copyright 2008-2010 John Smith`
- **SPDXID**: `SPDXRef-File`
- **FileComment**: `<text>The concluded license was taken from the p`
- **FileType**: `SOURCE`
- **FileChecksum**: `MD5: 624c1abb3664f4b35547e7c73864ad24`
- **FileChecksum**: `SHA1: d6a770ba38583ed4bb4525bd96e50461655d2758`
- **LicenseConcluded**: `(LGPL-2.0-or-later OR LicenseRef-2)`
- **LicenseInfoInFile**: `LicenseRef-2`

Snippets

- セクションの必須項目をまとめたスニペット呼び出し
 - Document Creation Information
 - Package Information
 - License Information

SPDX-Lite書きたい時に使える…?

```
16 ↓
17 ## Package Information ↓
18 PackageName: Software Package Name!
19 SPDXID: SPDXRef-Software Package Name!
20 PackageVersion: NOASSERTION!
21 PackageDownloadLocation: NOASSERTION!
22 FilesAnalyzed: false!
23 PackageHomePage: NOASSERTION!
24 PackageLicenseConcluded: NOASSERTION!
25 PackageLicenseDeclared: NOASSERTION!
26 PackageCopyrightText: <text></text>!
27 PackageComment: <text></text>!
28
```

Completion

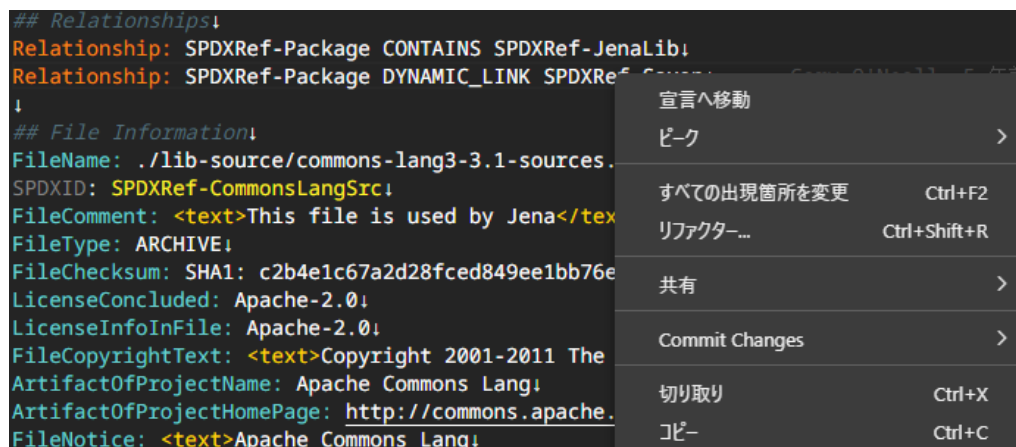
- 補完候補のリストアップ
 - SPDX ID(SPDXRef-〇〇)
 - License ID(LicenseRef-〇〇)

```
51 ## Package Information
52 PackageName: glibc
53 SPDXID: SPDXRef-
54 PackageVersion: SPDXRef-CommonsLangSrc
55 PackageFileName: SPDXRef-DoapSource
56 PackageSupplier: SPDXRef-DOCUMENT
57 PackageOriginat: SPDXRef-File
58 PackageDownload: SPDXRef-JenaLib
59 PackageVerifica: SPDXRef-Saxon
60 PackageChecksum: SPDXRef-Snippet
61 PackageChecksum: SHA256: 11b6d3ee554eedf79299
62 PackageChecksum: MD5: 624c1abb3664f4b35547e7c
63 PackageHomePage: http://ftp.gnu.org/gnu/glibc
```

Go to declaration

- ファイル内識別子の宣言位置へジャンプ
 - SPDX ID(SPDXRef-〇〇)
 - License ID(LicenseRef-〇〇)

```
## Relationships!
Relationship: SPDXRef-Package CONTAINS SPDXRef-JenaLib!
Relationship: SPDXRef-Package DYNAMIC_LINK SPDXRef-Source!
!
## File Information!
FileName: ./lib-source/commons-lang3-3.1-sources.jar
SPDXID: SPDXRef-CommonsLangSrc!
FileComment: <text>This file is used by Jena</text>
FileType: ARCHIVE!
FileChecksum: SHA1: c2b4e1c67a2d28fced849ee1bb76e
LicenseConcluded: Apache-2.0!
LicenseInfoInFile: Apache-2.0!
FileCopyrightText: <text>Copyright 2001-2011 The
ArtifactOfProjectName: Apache Commons Lang!
ArtifactOfProjectHomePage: http://commons.apache.org/
FileNotice: <text>Apache Commons Lang!
```



Check Syntax Errors

- 構文チェック
- まだ基本的な規則のみ

- 単一行

```
58 AnnotationComment: <text>File level annotation</text>
59 AnnotationType: This line need value. .spdx
60 SPDXREF: SPDX
61 ## Package In 問題の表示 (Alt+F8) 利用できるクイックフィックスはありません
62 PackageName: ↓
63 SPDXID: SPDXRef-Package↓
64 PackageVersion: 2.11.1↓
65 PackageFileName: glibc-2.11.1.tar.gz↓
66 PackageSupplier: Person: Jane Doe (jane.doe@example.
67 PackageOriginator: Organization: ExampleCodeInspect
```

- 複数行

```
FileNotice: <text>Apache Commons Lang!
Copyright 2001-2011 The Apache Software Foundation!
↓
This product includes software developed by:
The Apache Software Foundation (http
↓
This product includes software from
under the Apache License 2.0 (see: StringUtils.containsWhitespace())!
FileContributor: Apache Software Foundation!
```

4. 開発・OSS化経緯

なんで作ろうと思ったか？

「欲しいのに存在しなかったから。」

- 一番欲しかったのはシンタックスハイライトとジャンプ機能。
- 調べたら作り方が想像出来たので「やってみるかー」
- 技術的にも今後活きる経験になりそう。
 - 構文解析の仕組み
 - JavaScript(Node.js)のエコシステム

なんでOSS化しようと思ったか？

「同じように欲しいと思う人いそう。」

- まだ世の中に同じものは(おそらく)存在しない。
 - 「シンタックスハイライトあるだけでも便利では？」
 - 自分だけ抱えるには勿体ない。
- 発端がオープンソースの成果物でもあるし、これを公開することは“貢献”になるかも…

SPDX Specificationについて

- 公式OSSのサンプルがSpecificationに書いてあることと違う。
 - 例: `<text></text>`でvalue部分を挟んでない。
- “Information”と”Intelligence”が混ざってると混乱しない？
 - 例: LicenseDeclaredは宣言されているライセンス情報、つまり”伝え聞いたまま”の情報なのに対し、LicenceConcludedは結論づけられたライセンス情報、つまり”人の解釈を含めた”情報

※自分の解釈が間違ってる可能性もあります。

開発について

- 設計、コードの書き方を良くしようとするとう開発が全く進まない。
→ 形にすることを優先、歯を食いしばり無視することにした。

社内手続きについて

- 既存制度に沿うとコストのかけ方が実情に合わない気がする。
 - 例： 名前決めるのに数か月
- そもそも前例、制度がない部分があり、コネがない人はOSS化を進めることすら難しい。

渡邊さんのお力がなければ
無理でした

※個人の意見です。

社内の反応

- “偉い人”含め割と好印象、協力的な場合が多かった。
 - 動くモノを最初に見せた、内容が分かりやすい部類だったのが功を奏したかも。
- 気にするポイントはやっぱり「会社になんな影響があるか？」
 - 良い側面、悪い側面両方を説明する責任は生じる。
- 前例がなくとも、何とか形にして手続きしてくれることも。

※個人の意見です。

5. おわりに

リポジトリ、使い方

有り体で出してるので、温かい目で...

- ↓にインストール用パッケージ、ソースコード(MIT)。
 - <https://github.com/OLSV-oss/editor-for-sbom>
 - /build/editor-for-sbom-0.1.1.vsixをダウンロードした後はデモと同じ手順でインストール可
- 使い方は弊社のOSS管理ブログ↓に。
 - <https://www.hitachi-solutions.co.jp/oms/sp/blog/2023020101/>
 - 続報あれば基本この管理ブログで告知する予定

今後の開発に関する予定

- 開発のモチベーションはあるが、どれだけ出来るかは不明
 - 基本は業務の空き時間で実装する方針
 - 要望来たら検討はする
- 実装したいこと(≠予定)
 - 構文規則の追加
 - SPDX License Listにあるライセンス判別するとか、情報表示するとかさせたい...

END



2023/02/09

株式会社日立ソリューションズ
ITプラットフォーム事業部 デジタルシフト開発支援本部
プロセス改善ソリューション部 OSS管理ソリューショングループ

明石 知泰