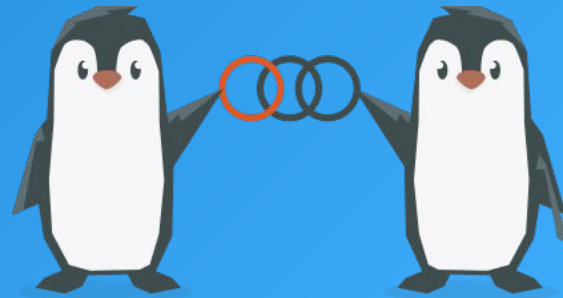


Introducing OpenChain Japan SBOM subgroup

2023/07/11



Breakout Session Schedule

参加者の皆様へ

質問などは随時コメントにご記載ください。
発言したい方は挙手 (ボタン)をお願いします。

- | | | |
|----|--|-------|
| 1. | SBOMサブグループの紹介 | 5min |
| | ルネサスエレクトロニクス(株) 伊藤 義行 | |
| 2. | SPDX Lite v2.3 の紹介とこれから | 10min |
| | オリンパス(株) 小泉 悟 | |
| 3. | SPDX v3.0 の紹介 と SPDX WG Community 参加のお誘い | 15min |
| | サイバートラスト(株) 富田 佑実 | |
| | ソニーグループ (株) 小保田 規生 | |

SBOMサブグループの紹介

- 概要

SBOMサブグループでは、以下の活動を行っています。

- SBOMIに関する話題を日本コミュニティメンバーに広く共有する、勉強する。
- OSSライセンス順守とセキュリティ観点の両方から、日本の産業界にとって使いやすい SBOMIについて議論する。
- SPDX WGと協力し、SBOM仕様を提案・実装する。

- [SPDX Lite](#)

OSSライセンス順守面から必要最小限となる項目は何かを議論し、SPDX WGに提案。

SPDX v2.2からSPDX仕様のAppendixとして採用されています。

SBOMサブグループの紹介



- SBOMサブグループの情報を得るには

- Github

[OpenChain-JWG/subgroups/sbom-sg at master · OpenChain-Project/OpenChain-JWG · GitHub](#)

- Slack

- OpenChain JWG Slackに参加

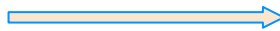
https://join.slack.com/t/openchain-japanwg/shared_invite/zt-1jf0n0zrb-u77QDi9QAOFnoZzU40hA4A

- 公開チャネル #10_sbom-sg に参加

<https://openchain-japanwg.slack.com/archives/CGDAB378R>

- ML

japan-sg-sbom@lists.openchainproject.org | Home



Group Email Addresses

Post: japan-sg-sbom@lists.openchainproject.org

Subscribe: japan-sg-sbom+subscribe@lists.openchainproject.org

Unsubscribe: japan-sg-sbom+unsubscribe@lists.openchainproject.org

Group Owner: japan-sg-sbom+owner@lists.openchainproject.org

Help: japan-sg-sbom+help@lists.openchainproject.org

- SBOMサブグループの会議に参加するには

- **MLおよびSlackのSBOM sg Channelで開催を案内**します。通常は **Automation sg**と2週に1回合同開催。Teamsの会議招待が MLに送られます。

SPDX Liteの紹介とこれから

別の資料で説明します！

SPDX 3.0 の変更点

Why SPDX 3.0?

Interest in SPDX for non-licensing scenarios **Security Vulnerability**

- supporting security and safety critical application compliance requirements. セキュリティの脆弱性や安全性が重要視されるコンプライアンス要件のサポート
- AI/ML and datasets increasing need for transparency AI/MLとデータセットにおける透明性の必要性の高まり

Consolidate efforts between the SPDX community & OMG/CISQ efforts. SPDXコミュニティとOMG/CISQの取り組みの統合

Reorganize enable general SBOM use cases, with minimum overhead 最小限のオーバーヘッドで有効なSBOMユースケースを再編成

Support optional inclusion properties for specific profiles: Licensing, Security, AI/ML Applications, Datasets, Build, Usage, ... 特定のプロファイルのための任意で含まれるプロパティをサポート

Open Source Summit North America 2023

Open Source Summit North America 2023

SPDX 3.0 Tooling Mini Summit

Video: [SPDX 3.0 Overview](#)



目的の違い

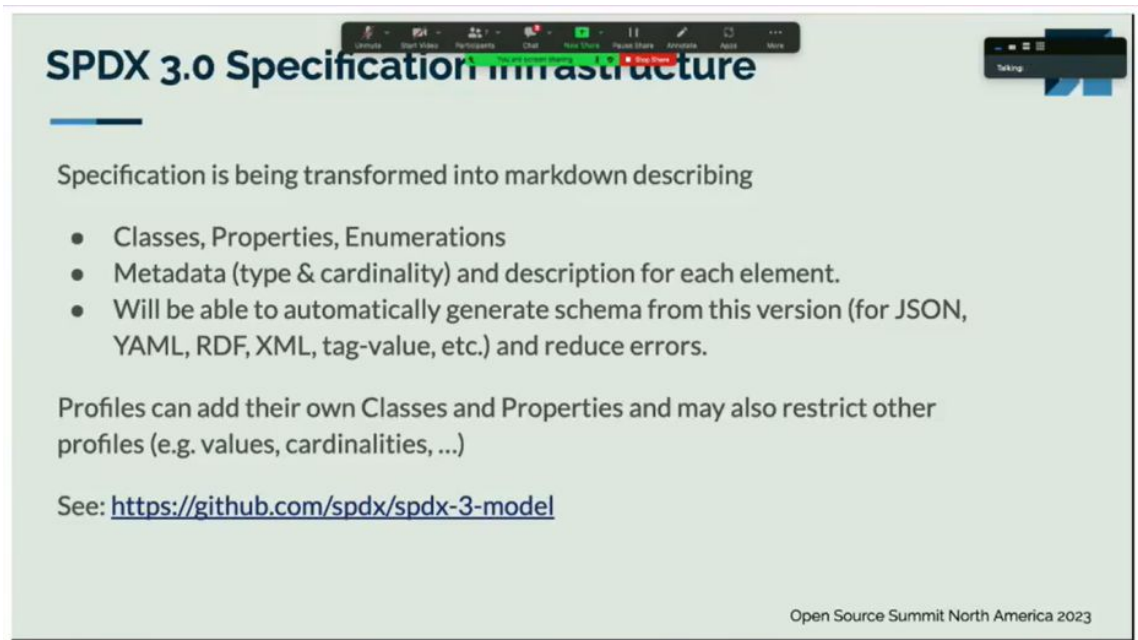
v2.3まで

- 主に、OSSライセンスコンプライアンス観点、脆弱性情報へのリンクは可能

v3.0から

- セキュリティの脆弱性とソフトウェアの高い信頼性と安全性
- AI/MLとデータセットの透明性

SPDX 3.0 の変更点



The screenshot shows a presentation slide with the title "SPDX 3.0 Specification infrastructure". Below the title, it states "Specification is being transformed into markdown describing" and lists three bullet points: "Classes, Properties, Enumerations", "Metadata (type & cardinality) and description for each element.", and "Will be able to automatically generate schema from this version (for JSON, YAML, RDF, XML, tag-value, etc.) and reduce errors." It then says "Profiles can add their own Classes and Properties and may also restrict other profiles (e.g. values, cardinalities, ...)" and provides a link to "https://github.com/spdx/spdx-3-model". At the bottom right, it says "Open Source Summit North America 2023".

SPDX 3.0 Specification infrastructure

Specification is being transformed into markdown describing

- Classes, Properties, Enumerations
- Metadata (type & cardinality) and description for each element.
- Will be able to automatically generate schema from this version (for JSON, YAML, RDF, XML, tag-value, etc.) and reduce errors.

Profiles can add their own Classes and Properties and may also restrict other profiles (e.g. values, cardinalities, ...)

See: <https://github.com/spdx/spdx-3-model>

Open Source Summit North America 2023

Open Source Summit North America 2023

SPDX 3.0 Tooling Mini Summit

Video: [SPDX 3.0 Overview](https://github.com/spdx/spdx-3-model) github: <https://github.com/spdx/spdx-3-model>



仕様に関する構造の違い

v2.3まで

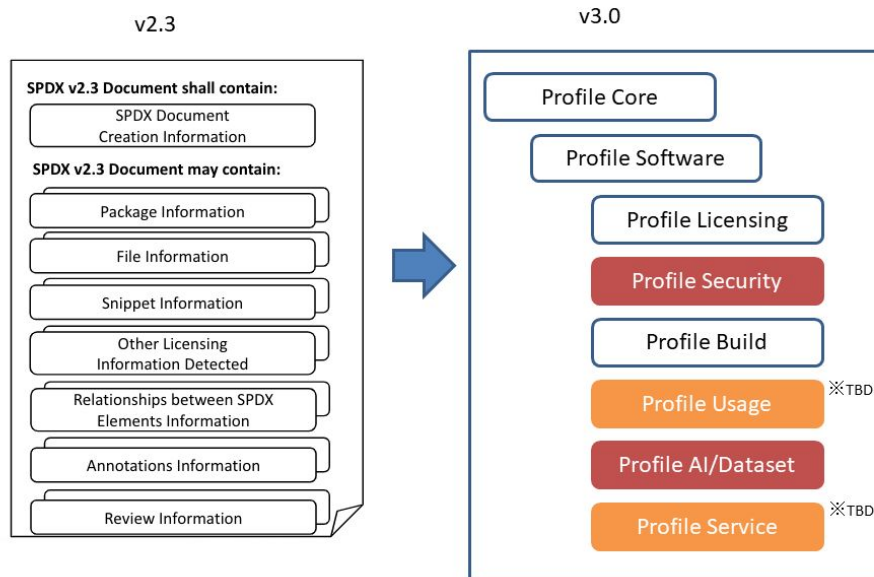
- **Tag - Value** の組み合わせ定義と、Valueに何を記載すべきかという仕様

v3.0から

- クラスとプロパティで定義される**オブジェクトモデル**
- **Profileが定義**され、**各クラス、プロパティをカスタマイズ**することが可能

SPDX 3.0の変更点

Changes from v2.3 to v3.0



- Security、AI/Dataset Profile が追加され、パッケージ情報やライセンス情報は、Software、Licensing Profileに分離
- Usage 、Service Profileについては議論中
- Lite ProfileもJWG SBOM sgから提案中

https://github.com/OpenChain-Project/OpenChain-JWG/blob/master/subgroups/sbom-sg/meetings/20230314/SPDX_version_comparison_en.pptx
を少し修正

SPDX 3.0の変更点

Structural Changes

Profiles

- Conformance Requirements 適合要件
 - Additional restrictions on properties (e.g. required license information in the licensing profile)
プロパティへの追加の制約事項
(例: licensing profileにおける必須ライセンス情報)
- Namespace 名前空間
 - Organizes the vocabulary into more logical digestible units (e.g. you don't have to know all the licensing terms if you're only interested in security)
論理的に消化可能な単位に語彙を整理する
(例: セキュリティのみに関心がある場合ライセンスに関するすべての用語を知っている必要はない)
- Organization
 - SPDX work groups are organized around profiles
SPDX WGがprofile周りを整理する



Open Source Summit North America 2023

Open Source Summit North America 2023

SPDX 3.0 Tooling Mini Summit

Video: 2.3 VS 3.0 Comparison Overview



Profiles

2つの意味を持っているため少し分かり辛い

- プロファイルごとに、各クラスの**プロパティの使い方に制約を加える** (プロファイルごとに必須要素を分ける、など)
- プロファイルごとに**名前空間を区切る** (セキュリティに関する情報だけを利用する、など)

SPDX 3.0 の議論

SPDX 2.3から大きく仕様が変わるため、SPDX WGは各サブグループごとに以下のようなスケジュールでオンラインミーティングを行っています。夜間開催となるミーティングもあり、日本からは少し参加しにくいかもしれませんが、興味のある話題には参加すると面白いと思います。

SPDX meetings (EST/EDT表記なので、大体AM00:00-とかAM01:00- JST)

<https://github.com/spdx/meetings>

SPDX-{tech, defects} ML (技術的な話題はこの2つのMLをフォローしておきましょう)

<https://lists.spdx.org/g/Spdx-tech>

<https://lists.spdx.org/g/spdx-defects>

SPDX Asia Telco.

毎月第2火曜日 朝9:00- on Zoom

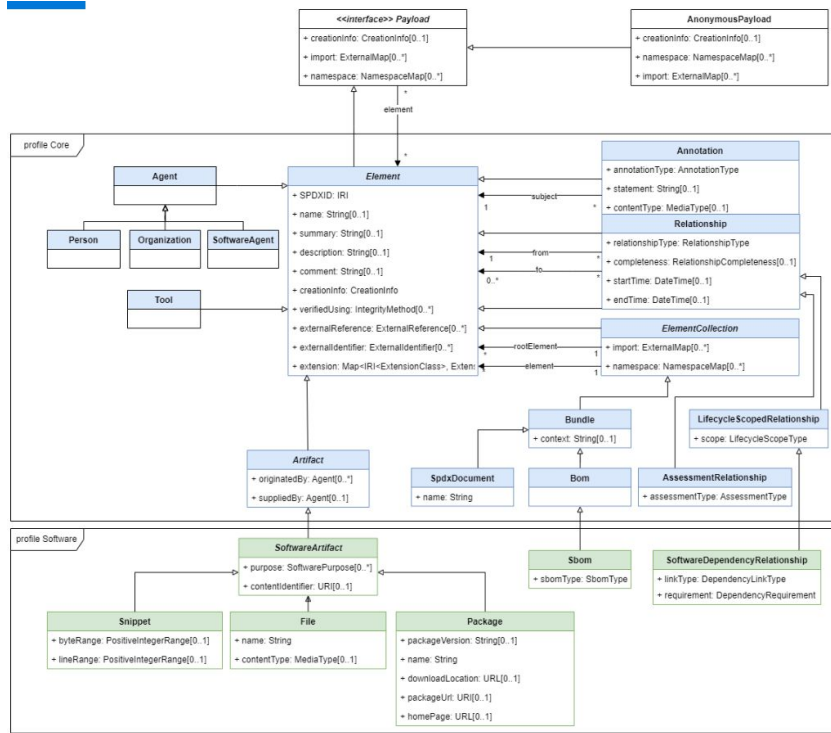
必要な方はML or Slackでご連絡ください。会議招待を送ってもらいます。



THE
LINUX
FOUNDATION



[spdx-3-model/model.png](https://spdx.org/licenses/spdx-3-model.png) at
cb37ac018d464cabcc11d4b590c7830a489c8f1f
5 · spdx/spdx-3-model (github.com)



クラスと各クラスが持つプロパティ、その関係が仕様化されています。

Licensing, Security などクラスが記載されていないProfileは、まだ仕様が煮詰まっていないものであり、それぞれ記載されている WGで議論が続いています。

これらクラス図は、draw.io を利用して作成されており、[このファイル](#)を利用することによって、VSCodeなどで編集することが出来ます。

SPDX 3.0 データタイプ

Simple Data Types

SemVer: String

String constrained to SemVer 2.0.0 specification.

MediaType: String

String constrained to RFC 2046 specification.

EmailAddress: String

String constrained to RFC 2822 specification.

Complex Data Types

These types have value/struct semantics - equality is determined by comparing values and they MUST NOT be referenced by name across documents. Serialization formats MAY enable de-duplication within a single document.

CreationInfo

- + specVersion: SemVer
- + profile: ProfileIdentifier[1..*]
- + created: DateTime
- + dataLicense: 'CC0'
- + createdBy: Agent[1..*]
- + createdUsing: Tool[0..*]
- + comment: String[0..1]

NamespaceMap

- + prefix: String
- + namespace: IRI

ExternalMap

- + externalId: IRI
- + locationHint: URL[0..1]
- + verifiedUsing: IntegrityMethod[0..*]

ExternalIdentifier

- + externalIdentifierType: ExternalIdentifierType
- + identifier: String
- + comment: String[0..1]

ExternalReference

- + externalReferenceType: ExternalReferenceType
- + locator: IRI
- + contentType: MediaType[0..1]
- + comment: String[0..1]

IntegrityMethod

- + comment: String[0..1]



Hash

- + algorithm: HashAlgorithm
- + hashValue: byte[1..*]

PositiveIntegerRange

- + start: PositiveInteger
- + end: PositiveInteger

ProfileIdentifier

- + name: String

ExtensionClass

Enumerations

RelationshipType

Meta
describes [bundle->artifact]
amends [element->element]
other [element->element] (comment)

Structure
contains [artifact->artifact]

Behavioral
dependsOn [artifact->artifact]
patches [artifact->artifact]
tests [artifact->artifact]

Pedigree
generates [artifact->artifact]
expandedFromArchive
fileAdded
fileDeleted
fileModified
copy [artifact->artifact]
packages (obsolete?)

Provenance
ancestor [artifact->artifact]
availableFrom[artifact->identity]
variant [artifact->artifact]

Obsolete?
buildTool
devTool
testTool
dependencyManifest
distributionArtifact
example
dataFile
testCase
documentation
metafile
test
requirementFor
specificationFor

RelationshipCompleteness

complete [Default]
incomplete
noAssertion

ExternalReferenceType

alDownloadLocation
alWebPageType
securityAdvisory
securityFix
securityOther
other

HashAlgorithm

sha1
sha224
sha256 [default]
sha384
sha512
sha3_224
sha3_256
sha3_384
sha3_512
md2
md4
md5
md6
spdx_pvc_sha1
spdx_pvc_sha256
blake2b_256
blake2b_384
blake2b_512
blake3
other

ExternalIdentifierType

cpe_2.2
cpe_2.3
email
purl
uri-scheme
swid (deprecated?)
swidid (deprecated?)
gitoid (deprecated?)
other

AnnotationType

review
other

SoftwarePurpose

application
archive
bom
configuration
container
data
device
documentation
executable
file
firmware
framework
install
library
module
operatingSystem
patch
source
other

DependencyLinkType

noAssertion [default]
static
dynamic
tool
other

DependencyScope

noAssertion [default]
build
dev
test
runtime
other

DependencyRequirement

noAssertion [default]
optional
required
provided
prerequisite

SbomType

TBD

各プロパティが持つデータの型の一覧と、データがとりうる範囲も仕様化されています。

Example: Package Information

例

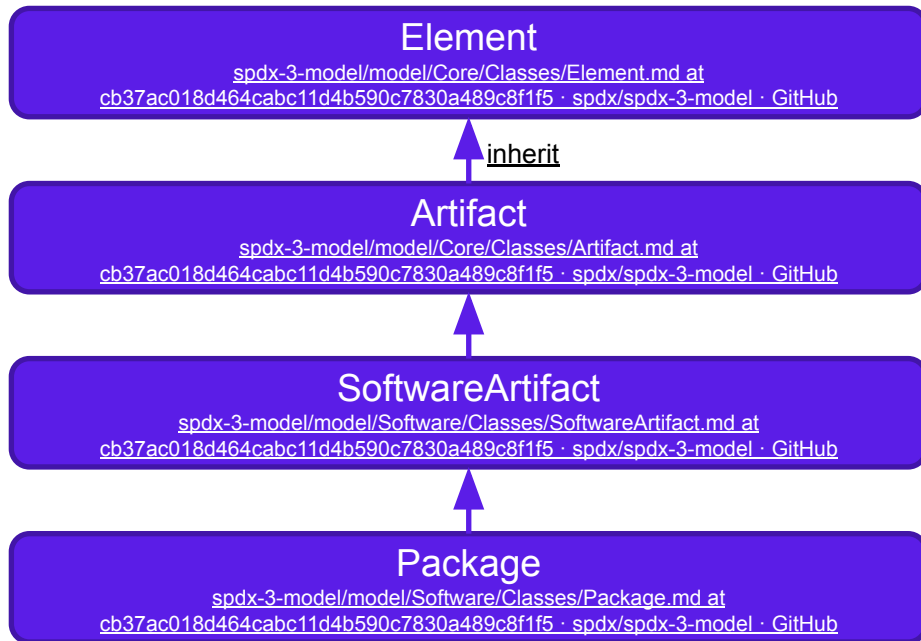
ソフトウェアパッケージに関する情報を
SBOMに含めたい場合

1. ソフトウェアパッケージの情報は、
Package Classが該当するはず！

Metadata

- name: Package
- SubclassOf: /Software/SoftwareArtifact

2. サブクラスになっているので、上位の抽象クラスを参照していく事になります。



Properties

Package

Properties

packageVersion
type: xsd:string
minCount: 0
maxCount: 1

downloadLocation
type: xsd:anyURI
minCount: 0
maxCount: 1

packageUri
type: xsd:anyURI
minCount: 0
maxCount: 1

homePage
type: xsd:anyURI
minCount: 0
maxCount: 1

sourceInfo
type: xsd:string
minCount: 0
maxCount: 1

SoftwareArtifact

Properties

contentIdentifier
type: xsd:anyURI
minCount: 0
maxCount: 1

primaryPurpose
type: SoftwarePurpose
minCount: 0
maxCount: 1

additionalPurpose
type: SoftwarePurpose
minCount: 0

concludedLicense
type: /Licensing/LicenseField
minCount: 0
maxCount: 1

declaredLicense
type: /Licensing/LicenseField
minCount: 0
maxCount: 1

copyrightText
type: xsd:string
minCount: 0
maxCount: 1

attributionText
type: xsd:string
minCount: 0
maxCount: 1

Artifact

Properties

originatedBy
type: Agent
minCount: 0

suppliedBy
type: Agent
minCount: 0

builtTime
type: DateTime
minCount: 0
maxCount: 1

releaseTime
type: DateTime
minCount: 0
maxCount: 1

validUntilTime
type: DateTime
minCount: 0
maxCount: 1

standard
type: xsd:string
minCount: 0

Element

Properties

spdxId
type: xsd:anyURI
minCount: 1
maxCount: 1

name
type: xsd:string
maxCount: 1

summary
type: xsd:string
maxCount: 1

description
type: xsd:string
maxCount: 1

comment
type: xsd:string
maxCount: 1

creationInfo
type: CreationInfo
minCount: 0
maxCount: 1

verifiedUsing
type: IntegrityMethod

externalReference
type: ExternalReference
minCount: 0

externalIdentifier
type: ExternalIdentifier
minCount: 0

extension
type: Extension
minCount: 0

3. SBOMに含まれるソフトウェアパッケージの情報は、左にある全てのプロパティ集合となります。

各プロパティの詳細

SBOM

spdx-3-model/model/Software/Classes/Sbom.md at [cb37ac018d464cab11d4b590c7830a489c8f1f5](https://github.com/spdx/spdx-3-model) · [spdx/spdx-3-model](https://github.com/spdx/spdx-3-model) · [GitHub](https://github.com)

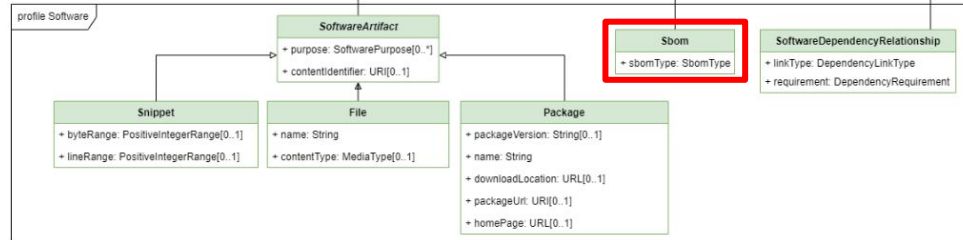
Properties

sbomType

type: SBOMType

minCount: 0

4. プロパティの詳細は、model/各プロファイル/Propertiesの下にmarkdownファイルとして存在しています。
例えば、Software ProfileのSBOMクラスに含まれるsbomTypeというプロパティは、/model/Software/Properties/sbomType.mdに説明が記載されています。



SPDX-License-Identifier: Community-Spec-1.0

sbomType

Summary

Provides information about the type of an SBOM.

Description

This field is a reasonable estimation of the type of SBOM created from a creator perspective. It is intended to be used to give guidance on the elements that may be contained within it. Aligning with the guidance produced in [Types of Software Bill of Material \(SBOM\) Documents](#).

Metadata

- name: sbomType
- Nature: DataProperty
- Range: SBOMType

spdx-3-model/model/Software/Properties/sbomType.md at [cb37ac018d464cab11d4b590c7830a489c8f1f5](https://github.com/spdx/spdx-3-model) · [spdx/spdx-3-model](https://github.com/spdx/spdx-3-model) · [GitHub](https://github.com)

各プロパティに設定する値の範囲

SBOMType

Summary

Provides a set of values to be used to describe the common types of SBOMs that tools may create.

Description

The set of SBOM types with definitions as defined in [Types of Software Bill of Material \(SBOM\) Documents](#), published on April 21, 2023. An SBOM type describes the most likely type of an SBOM from the producer perspective, so that consumers can draw conclusions about the data inside an SBOM. A single SBOM can have multiple SBOM document types associated with it.

Metadata

- name: SBOMType

Entries

- design: SBOM of intended, planned software project or product with included components (some of which may not yet exist) for a new software artifact.
- source: SBOM created directly from the development environment, source files, and included dependencies used to build an product artifact.
- build: SBOM generated as part of the process of building the software to create a releasable artifact (e.g., executable or package) from data such as source files, dependencies, built components, build process ephemeral data, and other SBOMs.
- deployed: SBOM provides an inventory of software that is present on a system. This may be an assembly of other SBOMs that combines analysis of configuration options, and examination of execution behavior in a (potentially simulated) deployment environment.
- runtime: SBOM generated through instrumenting the system running the software, to capture only components present in the system, as well as external call-outs or dynamically loaded components. In some contexts, this may also be referred to as an "Instrumented" or "Dynamic" SBOM.
- analyzed: SBOM generated through analysis of artifacts (e.g., executables, packages, containers, and virtual machine images) after its build. Such analysis generally requires a variety of heuristics. In some contexts, this may also be referred to as a "3rd party" SBOM.

5. プロパティはKey – Value となっていますが、その Value側に取りうる範囲を制限する場合には、Vocabulariesが設定されています。とりうる値の範囲についての説明は、model/各プロファイル/Vocabulariesの下にmarkdownファイルとして存在しています。

[spdx-3-model/model/Software/Vocabularies/SBOMType.md at cb37ac018d464cab11d4b590c7830a489c8f1f5 · spdx/spdx-3-model · GitHub](#)

Thank you !

