EOSC
ETRI Open Source Center

OpenChain-KWG Tooling SG 회의('23년 8월)

SPDX Tools 사용법

2023.8.9.(수)

ETRI 오픈소스센터
박정숙

참고자료

- 오픈소스 컴플라이언스 관련 도구 리스트: https://oss-compliance-tooling.org/Tooling-Landscape/OSS-Based-License-Compliance-Tools/
- SPDX website: https://spdx.dev/
- SPDX Tools, https://github.com/spdx/tools
- SPDX Specification, https://github.com/spdx/spdx-spec
- ISO/IEC 5962:2021, “Information technology – SPDX Specification V2.2.1”, https://www.iso.org/standard/81870.html
- LF, “SPDX Announces 3.0 Release Candidate with New Use Cases”, https://www.linuxfoundation.org/press/spdx-sbom-3-release-candidate

내용

- 개요
- SBOM 포맷 규격들 비교
- SPDX V2.3 필드 분석
- SPDX Tools 사용법
- SPDX 3.0 개발 현황
- 마무리

개요

- **최근 SW 보안 위협이 급증하면서 이에 SBOM의 중요성 증가 중**
- **SBOM 규격으로는 SPDX, CycloneDX, SWID 등 고려**
  - ➢SPDX, SWID는 국제 표준임
  - ➢규격이 SW 공급망 정보를 잘 표현하고 있는지가 관건
    - ✓의존성, 보안취약점
- **본 발표는 SPDX Tools의 개발 상태 확인이 목표**

SBOM 포맷

- **SBOM 포맷**
  - SBOM 생성을 위한 통합 구조를 정의하고 최종 사용자 또는 고객과 공유하기 위한 표준
  - SW의 구성을 다른 툴이 이해가능하도록 공통의 형식으로 설명
- **종류**
  - SPDX(Software Package Data Exchange)
  - CycloneDX
  - SWID(Software Identification Tags)

SBOM 포맷 규격들 비교 – CycloneDX

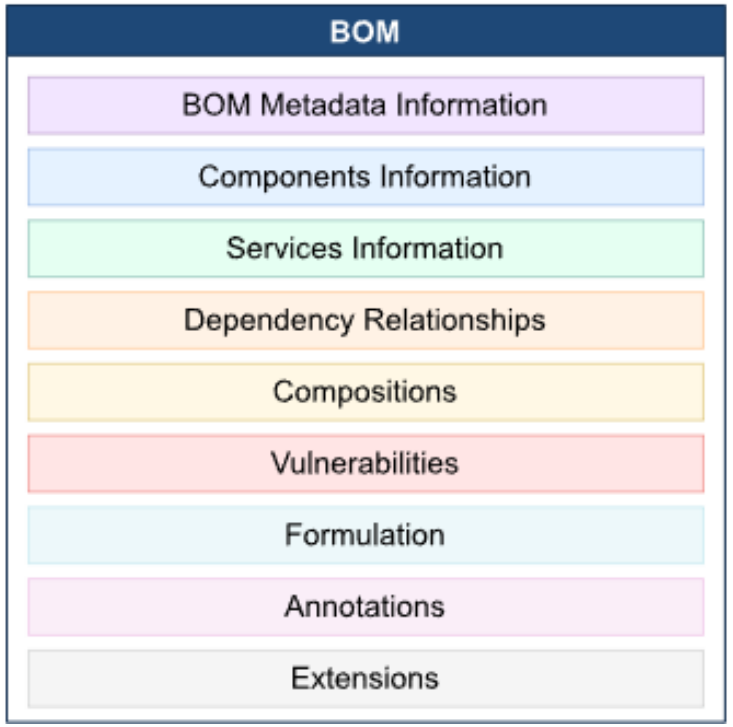
- 국제 웹 보안 표준 기구(OWASP)이 주도
- 애플리케이션 보안 컨텍스트 및 공급망 구성 요소 분석에 사용하도록 설계된 경량의 SBOM 표준

SBOM 포맷 규격들 비교 – CycloneDX

- 참고: https://cyclonedx.org/specification/overview/

- JSON Schema, XML Schema로 정의
- Protocol Buffers는메타데이터, 컴포넌트, 서비스, 의존성, 구성, 의존성으로 구성
- 규범적이고 사용 편리
- SBOM, SaaSBOM, OBOM, MBOM, VEX 유즈케이스를 위해 설계
- 복잡한 관계 쉽게 설명
- 특수화된 또는 향후 사용 사례를 지원하도록 확장 가능

- SWID 참고
  - https://csrc.nist.gov/Projects/Software-Identification-SWID/guidelines



SBOM 포맷 규격들 비교 – CycloneDX

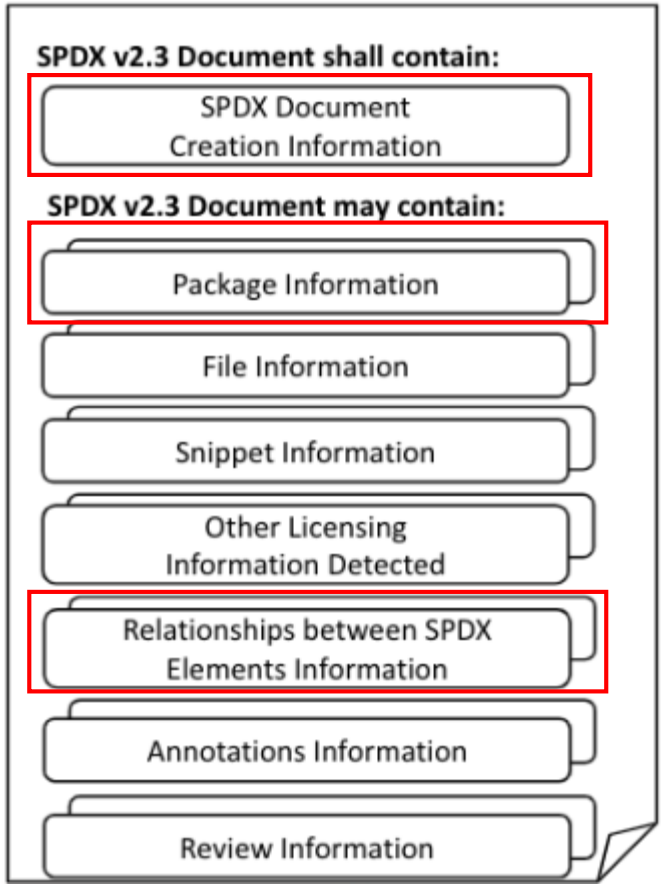
- 세부 필드 설명

SBOM 포맷 규격들 비교 – SPDX

- **SPDX란?**
  - ➢LF SPDX Project에서 개발 중인 SW 패키지와 관련된 구성 요소, 라이선스 및 저작권을 전달하기 위한 표준 형식
  - ➢ISO/IEC 표준: SPDX V2.2.1과 동일
    - ✓ISO/IEC 5962:2021
    - ✓https://www.iso.org/standard/81870.html

SPDX V2.3 필드 분석

- **구성**
  - ➢SPDX Document Creation
    - ✓분석 툴 이용 시 이후 또는 이전 버전과의 호환성 표시
  - ➢Package
    - ✓제품, 컨테이너 및 구성요소와 같은 다양한 개체 설명
    - ✓컨텍스트를 공유하는 항목들을 그룹화
  - ➢File
    - ✓이름, 체크섬, 라이선스, 저작권 정보 등의 파일 메타 데이터
  - ➢Snippet(선택)
    - ✓데이터가 다른 원본에서 유도 또는 다른 라이선스와 관련 시 주로 사용
  - ➢Relationships between SPDX elements
    - ✓문서, 패키지, 파일에 대한 관계 표시
  - ➢Annotation
    - ✓검토자의 검토 활동 정보 기록



SPDX V2.3 필드 분석 – Document creation information

필드명	설명	표기법
SPDX version	SPDX 포맷의 버전 번호	SPDX-2.3
Data license	본 문서의 라이선스	CC0-1.0
SPDX identifier	다른 파일, 내부 패키지 및 외부 문서와의 관계에서 참조가능한 현재 SDPX 문서	SPDXRef-DOCUMENT
Document name	문서 명칭	프로젝트명 (버전 정보 표기 방법은?)
SPDX document namespace	절대 URI로 SPDX 문서별 네임스페이스 제공 (RFC-3986 준수)	https://spdx.org/spdxdocs/spdx-tools-v1.2-3F2504E0-4F89-41D3-9A0C-0305E82...
External document references	이 SPDX 문서 내에서 참조되는 모든 외부 SPDX 문서 식별	DocumentRef-spdx-tool-1.2 https://spdx.org/spdxdocs/spdx-tools-v1.2-3F2504E0-4F89-41D3-9A0C-0305E82C3301 SHA1: d6a770ba38583ed4bb4525bd96e50461655d2759
License list version	문서 생성 시 사용된 SPDX 라이선스 목록의 버전 제공. 라이선스가 각 후속 버전과 함께 SPDX 라이선스 목록에 추가됨을 인식하여 SPDX 문서의 수신자에게 사용된 SPDX 라이선스 목록의 버전을 제공하는 것이 목적	3.17
Creator	SPDX 문서 생성자 식별. SPDX 문서가 SW 도구 사용으로 생성된 경우 해당 도구의 이름과 버전 표시	Creator: Person: Jane Doe () Creator: Organization: ExampleCodeInspect () Creator: Tool: LicenseFind-1.0
Created	SPDX 문서가 처음 생성된 시기 식별 (UTC 형식)	2010-01-29T18:30:22Z
Creator comment	SPDX 문서 생성에 대한 일반적 설명 또는 다른 필드에 포함 안된 기타 관련 설명 제공 문서 수신자에게 문서 작성자의 의견을 제공하기 위함	<text>This SPDX document was created by a combination of using a free tool, as indicated above, and manual analysis by several authors of the code.</text>
Document comment	문서 콘텐츠 작성자가 SPDX 문서 소비자에게 설명을 제공하는 선택적 필드	DocumentComment: <**text**>This document was created **using** SPDX 2.3, version 3.17 **of** the SPDX License List and refering **to** licenses **in** file MyCompany.Approved.Licenses.spdx.</**text**>

SPDX V2.3 필드 분석– Package information

필드명	설명	표기법
Package name	패키지명	
Package SPDX identifier	고유한 값	SPDXRef-Package-〈숫자〉
Package version	패키지 버전	
Package file name	패키지의 실제 파일 이름 또는 패키지로 취급되는 디렉토리 경로	PackageFileName: glibc-2.11.1.tar.gz PackageFileName: ./myrootdir/mysubdir1
Package supplier	웹사이트가 아닌 조직 또는 인정된 작성자	Jane Doe (jane.doe@example.com)
Package originator	식별된 패키지가 공급업체로 식별된 것과 다른 사람 또는 조직에서 유래된 경우 패키지가 원래 어디서 왔는지 또는 누구로부터 왔는지 식별	ExampleCodeInspect (contact@example.com)
Package download location	다운로드 URL 또는 SPDX 문서가 생성된 시점의 패키지에 대한 VCS 내의 특정위치 식별	http://ftp.gnu.org/gnu/glibc/glibc-ports-2.15.tar.gz
Files analyzed	이 패키지의 파일 내용이 분석에 사용가능한지 또는 분석 대상인지 나타냄	False/ true
Package verification code	패키지를 구성하는 실제 파일에서 패키지의 특정 내용을 식별하는 독립적으로 재생가능한 메커니즘 제공	d6a770ba38583ed4bb4525bd96e50461655d2758
Package checksum	특정 패키지의 고유한 식별을 허용하는 독립적으로 재현가능한 메커니즘 제공	SHA1: 85ed0817af83a24ad8da68c2b5094de69833983c
Package homepage	패키지 홈페이지	http://ftp.gnu.org/gnu/glibc
Source information	관련 배경 정보나 패키지 출처에 대한 추가 의견 기록	<text>uses glibc-2_11-branch from git://sourceware.org/git/glibc.git.</text>
Concluded license	지배적인 라이선스를 결정할 수 없는 경우 SPDX 문서 작성자가 패키지 또는 대체값을 지배하는 것으로 결론을 내린 라이선스	LGPL-2.1-only
All licenses information from files	패키지에 있는 모든 라이선스들	LGPL-2.1-only, LicenseRef-1, LicenseRef-2

출처: https://spdx.github.io/spdx-spec/v2.3/package-information/#76-package-originator-field

SPDX V2.3 필드 분석– Package information

필드명	설명	표기법
Declared license	패키지 작성자가 선언한 라이선스 나열	GPL-2.0-only AND LicenseRef-3
Comments on license	패키지에 대한 Concluded License에 도달하기 위해 들어간 관련 배경 정보 또는 분석을 기록할 수 있는 장소를 제공	<text>The license for this project changed with the release of version 1.4. The version of the project included here post-dates the license change.</text>
Copyright text	패키지의 저작권 소유자와 날짜 확인	<text>Copyright 2008-2010 John Smith</text>
Package summary description	패키지에 대한 간단한 설명	<text>GNU C library.</text>
Package detailed description	패키지에 대한 자세한 설명	<text>The GNU C Library defines functions that are specified by the ISO C standard, as well as additional features specific to POSIX and other derivatives of the Unix operating system, and extensions specific to GNU systems.</text>
Package comment	문서 작성자가 설명 중인 패키지에 대한 일반적인 의견 기록	The package includes several sub-packages; see Relationship information.
External reference	패키지와 관련된다고 생각되는 추가 정보, 메타데이터, 열거, 자산식별자 또는 다운로드 가능한 콘텐츠의 외부소스 기재 예: 알려진 보안취약점이 있는 패키지를 식별하는 구조화된 명명 체계 (Spec Annex F. 참고)	SECURITY cpe23Type cpe:2.3:a:pivotal_software:spring_framework:4.1.0:*:*:*:*:*:*:*
External reference comment	참조의 목적과 대상에 대해 사람이 읽을 수 있는 정보 제공	<text>NIST National Vulnerability Database (NVD) describes security vulnerabilities (CVEs) which affect Vendor Product Version acmecorp:acmenator:6.6.6.</text>
Package attribution text	패키지 수준에서 일부 컨텍스트에서 전달해야 할 수 있는 승인 기록	All advertising materials mentioning features or use **of** this software must display the following acknowledgement: This product includes software developed **by** the AT&T.
Primary package purpose	패키지의 기본 용도	FRAMEWORK
Release date	패키지가 릴리즈된 날짜 기록	2010-01-29T18:30:22Z
Built date	패키지가 빌드된 실제 날짜	2010-01-29T18:30:22Z
Valid until date	공급자로부터 패키지 지원이 종료되는 날짜	2010-01-29T18:30:22Z

SPDX V2.3 필드 분석 – File information (필드 설명 생략)

필드명	설명	표기법
File name		
File SPDX identifier		
File type		
File checksum		
Concluded license		
License information in file		
Comments on license		
Copyright text		
Artifact of project name (deprecated)		
Artifact of project homepage (deprecated)		
Artifact of project uniform resource identifier (deprecated)		
File comment		
File notice		
File contributor		
File attribution text		
File dependencies (deprecated)		

SPDX V2.3 필드 분석 – Snippet information(필드 설명 생략)

필드명	설명	표기법
Snippet SPDX identifier		
Snippet from file SPDX identifier		
Snippet byte range		
Snippet line range		
Snippet concluded license		
License information in snippet		
Snippet comments on license		
Snippet copyright text		
Snippet comment		
Snippet name		
Snippet attribution text		

SPDX V2.3 필드 분석 – Other licensing information detected

필드명	설명	표기법
License identifier	SPDX 라이선스 목록에 없는 라이선스에 대해 사람이 읽을 수 있는 짧은 형식의 라이선스 식별자	LicenseRef-Whiskeyware
Extracted text	SPDX 라이선스 목록에 없는 라이선스에 대한 패키지, 파일, 스니펫에 있는 텍스트	<text>This software is licensed under the WHISKEY-WARE LICENSE.</text>
License name	라이선스 제목 또는 레이블로 사용하기에 적합한 사람이 읽을 수 있는 이름	Whiskey-Ware License
License cross reference	SPDX 라이선스 목록에 없는 라이선스의 정식 소스	http://people.freebsd.org/~phk/
License comment	라이선스 추가 정보를 SPDX 문서의 수신자에게 제공	The Whiskey-Ware License has a couple of other standard variants.

SPDX V2.3 필드 분석– Relationship between SPDX Elements Information

필드명	설명	표기법
Relationship	두 SPDX 요소 간의 관계에 대한 정보 제공	SPDXRef-grep CONTAINS SPDXRef-make SPDXRef-DOCUMENT AMENDS DocumentRef-SPDXA:SPDXRef-DOCUMENT SPDXRef-CarolCompression DEPENDS_ON NONE SPDXRef-BobBrowser CONTAINS NOASSERTION
Relationship comment	SPDX 문서의 두 요소 간의 관계를 분석한 후 결정된 추가 정보를 SPDX 문서 수신자에게 제공	The package foo.tgz is a pre-requisite for building executable bar.

SPDX V2.3 필드 분석: Relationship 종류(1/3)

Relationship	Description	Example
DESCRIBES	Is to be used when SPDXRef-DOCUMENT describes SPDXRef-A.	An SPDX document WildFly.spdx describes package 'WildFly'. Note this is a logical relationship to help organize related items within an SPDX document that is mandatory if more than one package or set of files (not in a package) is present.
DESCRIBED_BY	Is to be used when SPDXRef-A is described by SPDXREF-Document.	The package 'WildFly' is described by SPDX document WildFly.spdx.
CONTAINS	Is to be used when SPDXRef-A contains SPDXRef-B.	An ARCHIVE file bar.tgz contains a SOURCE file foo.c.
CONTAINED_BY	Is to be used when SPDXRef-A is contained by SPDXRef-B.	A SOURCE file foo.c is contained by ARCHIVE file bar.tgz
DEPENDS_ON	Is to be used when SPDXRef-A depends on SPDXRef-B.	Package A depends on the presence of package B in order to build and run
DEPENDENCY_OF	Is to be used when SPDXRef-A is dependency of SPDXRef-B.	A is explicitly stated as a dependency of B in a machine-readable file. Use when a package manager does not define scopes.
DEPENDENCY_MANIFEST_OF	Is to be used when SPDXRef-A is a manifest file that lists a set of dependencies for SPDXRef-B.	A file package.json is the dependency manifest of a package foo. Note that only one manifest should be used to define the same dependency graph.
BUILD_DEPENDENCY_OF	Is to be used when SPDXRef-A is a build dependency of SPDXRef-B.	A is in the compile scope of B in a Maven project.
DEV_DEPENDENCY_OF	Is to be used when SPDXRef-A is a development dependency of SPDXRef-B.	A is in the devDependencies scope of B in a Maven project.
OPTIONAL_DEPENDENCY_OF	Is to be used when SPDXRef-A is an optional dependency of SPDXRef-B.	Use when building the code will proceed even if a dependency cannot be found, fails to install, or is only installed on a specific platform. For example, A is in the optionalDependencies scope of npm project B.
PROVIDED_DEPENDENCY_OF	Is to be used when SPDXRef-A is a to be provided dependency of SPDXRef-B.	A is in the provided scope of B in a Maven project, indicating that the project expects it to be provided, for instance, by the container or JDK.
TEST_DEPENDENCY_OF	Is to be used when SPDXRef-A is a test dependency of SPDXRef-B.	A is in the test scope of B in a Maven project.
RUNTIME_DEPENDENCY_OF	Is to be used when SPDXRef-A is a dependency required for the execution of SPDXRef-B.	A is in the runtime scope of B in a Maven project.
EXAMPLE_OF	Is to be used when SPDXRef-A is an example of SPDXRef-B.	The file or snippet that illustrates how to use an application or library.

SPDX V2.3 필드 분석: Relationship 종류(2/3)

Relationship	Description	Example
GENERATES	Is to be used when SPDXRef-A generates SPDXRef-B.	A SOURCE file makefile.mk generates a BINARY file a.out
GENERATED_FROM	Is to be used when SPDXRef-A was generated from SPDXRef-B.	A BINARY file a.out has been generated from a SOURCE file makefile.mk. A BINARY file foolib.a is generated from a SOURCE file bar.c.
ANCESTOR_OF	Is to be used when SPDXRef-A is an ancestor (same lineage but pre-dates) SPDXRef-B.	A SOURCE file makefile.mk is a version of the original ancestor SOURCE file 'makefile2.mk'
DESCENDANT_OF	Is to be used when SPDXRef-A is a descendant of (same lineage but postdates) SPDXRef-B.	A SOURCE file makefile2.mk is a descendant of the original SOURCE file 'makefile.mk'
VARIANT_OF	Is to be used when SPDXRef-A is a variant of (same lineage but not clear which came first) SPDXRef-B.	A SOURCE file makefile2.mk is a variant of SOURCE file makefile.mk if they differ by some edit, but there is no way to tell which came first (no reliable date information).
DISTRIBUTION_ARTIFACT	Is to be used when distributing SPDXRef-A requires that SPDXRef-B also be distributed.	A BINARY file foo.o requires that the ARCHIVE file bar-sources.tgz be made available on distribution.
PATCH_FOR	Is to be used when SPDXRef-A is a patch file for (to be applied to) SPDXRef-B.	A SOURCE file foo.diff is a patch file for SOURCE file foo.c.
PATCH_APPLIED	Is to be used when SPDXRef-A is a patch file that has been applied to SPDXRef-B.	A SOURCE file foo.diff is a patch file that has been applied to SOURCE file 'foo-patched.c'.
COPY_OF	Is to be used when SPDXRef-A is an exact copy of SPDXRef-B.	A BINARY file alib.a is an exact copy of BINARY file a2lib.a.
FILE_ADDED	Is to be used when SPDXRef-A is a file that was added to SPDXRef-B.	A SOURCE file foo.c has been added to package ARCHIVE bar.tgz.
FILE_DELETED	Is to be used when SPDXRef-A is a file that was deleted from SPDXRef-B.	A SOURCE file foo.diff has been deleted from package ARCHIVE bar.tgz.
FILE_MODIFIED	Is to be used when SPDXRef-A is a file that was modified from SPDXRef-B.	A SOURCE file foo.c has been modified from SOURCE file foo.orig.c.
EXPANDED_FROM_ARCHIVE	Is to be used when SPDXRef-A is expanded from the archive SPDXRef-B.	A SOURCE file foo.c, has been expanded from the archive ARCHIVE file xyz.tgz.
DYNAMIC_LINK	Is to be used when SPDXRef-A dynamically links to SPDXRef-B.	An APPLICATION file 'myapp' dynamically links to BINARY file zlib.so.
STATIC_LINK	Is to be used when SPDXRef-A statically links to SPDXRef-B.	An APPLICATION file 'myapp' statically links to BINARY zlib.a.
DATA_FILE_OF	Is to be used when SPDXRef-A is a data file used in SPDXRef-B.	An IMAGE file 'kitty.jpg' is a data file of an APPLICATION 'hellokitty'.
TEST_CASE_OF	Is to be used when SPDXRef-A is a test case used in testing SPDXRef-B.	A SOURCE file testMyCode.java is a unit test file used to test an APPLICATION MyPackage.
BUILD_TOOL_OF	Is to be used when SPDXRef-A is used to build SPDXRef-B.	A SOURCE file makefile.mk is used to build an APPLICATION 'zlib'.

SPDX V2.3 필드 분석: Relationship 종류(3/3)

Relationship	Description	Example
DEV_TOOL_OF	Is to be used when SPDXRef-A is used as a development tool for SPDXRef-B.	Any tool used for development such as a code debugger.
TEST_OF	Is to be used when SPDXRef-A is used for testing SPDXRef-B.	Generic relationship for cases where it's clear that something is used for testing but unclear whether it's TEST_CASE_OF or TEST_TOOL_OF.
TEST_TOOL_OF	Is to be used when SPDXRef-A is used as a test tool for SPDXRef-B.	Any tool used to test the code such as ESlint.
DOCUMENTATION_OF	Is to be used when SPDXRef-A provides documentation of SPDXRef-B.	A DOCUMENTATION file readme.txt documents the APPLICATION 'zlib'.
OPTIONAL_COMPONENT_OF	Is to be used when SPDXRef-A is an optional component of SPDXRef-B.	A SOURCE file fool.c (which is in the contributors directory) may or may not be included in the build of APPLICATION 'atthebar'.
METAFILE_OF	Is to be used when SPDXRef-A is a metafile of SPDXRef-B.	A SOURCE file pom.xml is a metafile of the APPLICATION 'Apache Xerces'.
PACKAGE_OF	Is to be used when SPDXRef-A is used as a package as part of SPDXRef-B.	A Linux distribution contains an APPLICATION package gawk as part of the distribution MyLinuxDistro.
AMENDS	Is to be used when (current) SPDXRef-DOCUMENT amends the SPDX information in SPDXRef-B.	(Current) SPDX document A version 2 contains a correction to a previous version of the SPDX document A version 1. Note the reserved identifier SPDXRef-DOCUMENT for the current document is required.
PREREQUISITE_FOR	Is to be used when SPDXRef-A is a prerequisite for SPDXRef-B.	A library bar.dll is a prerequisite or dependency for APPLICATION foo.exe
HAS_PREREQUISITE	Is to be used when SPDXRef-A has as a prerequisite SPDXRef-B.	An APPLICATION foo.exe has prerequisite or dependency on bar.dll
REQUIREMENT_DESCRIPTION_FOR	Is to be used when SPDXRef-A describes, illustrates, or specifies a requirement statement for SPDXRef-B.	A PDF document that describes a list of disallowed licences to inherit in certain build-subtrees.
SPECIFICATION_FOR	Is to be used when SPDXRef-A describes, illustrates, or defines a design specification for SPDXRef-B.	A UML diagram illustrating a directed requirement graph for a discernible set of software components in a software package.
OTHER	Is to be used for a relationship which has not been defined in the formal SPDX specification. A description of the relationship should be included in the Relationship comments field.	

SPDX V2.3 필드 분석 – Annotation information

필드명	설명	표기법
Annotator field	모호한 스니펫, 파일 및 패키지에 대한 정보를 확인하고 추가	Person: Jane Doe
Annotation date field	댓글이 작성된 시기 식별	2010-01-29T18:30:22Z
Annotation type field	주석 유형 기록	REVIEW
SPDX identifier reference field	참조 중인 SPDX 문서의 요소를 고유하게 식별	SPDXRef-45 DocumentRef-spdx-tool-1.2:SPDXRef-5
Annotation comment field	분석에 대한 설명 제공	<text>All of the licenses seen in the file, are matching what was seen during manual inspection. There are some terms that can influence the concluded license, and some alternatives may be possible, but the concluded license is one of the options.</text>

SPDX Tools 사용법

- **SPDX Tools**
  - LF SPDX Project에서 SPDX 포맷 생성, 포맷 변경을 위해 지원하는 도구
  - 상세한 사용법은 https://github.com/spdx/tools 참고
- **사용법**
  - SPDX format converters
    - ✓ TagToSpreadsheet, TagToRDF, RdfToTag, RdfToHtml, RdfToSpreadsheet, SpreadsheetToRDF, SpreadsheetToTag 활용 가능
    - ✓ TagToRDF
      - ❖ java –jar spdx-tools-jar-with-dependencies.jar TagToRDF Examples/SPDXTagExample.tag TagToRDF.rdf
  - java –jar spdx-tools-jar-with-dependencies.jar 〈function〉 〈parameters〉
    - ✓ CompareSpdxDocs
      - ❖ java –jar spdx-tools-jar-with-dependencies.jar CompareSpdxDocs doc1 doc2 [output]
    - ✓ CompareMultipleSpdxDocs
      - ❖ java –jar spdx-tools-jar-with-dependencies.jar CompareMultipleSpdxDocs output.xls doc1 doc2 … docN
    - ✓ SPDXViewer
      - ❖ java –jar spdx-tools-jar-with-dependencies.jar SPDXViewer TestFiles/SPDXRdfExample.rdf
    - ✓ Verify
      - ❖ java –jar spdx-tools-jar-with-dependencies.jar Verify TestFiles/SPDXRdfExample.rdf
    - ✓ GenerateVerificationCode sourceDirectory
      - ❖ java –jar spdx-tools-jar-with-dependencies.jar GenerateVerificationCode sourceDirectory [ignoredFilesRegex]
  - SPDX Validation Tool

SPDX 3.0 개발 현황

- **최근 미국 정부(EO 14028)와 유럽 연합(Cyber Resiliency Act)이 SW 종속성과 공급망을 보호하기 위해 노력함에 따라 실행 가능하고 사용가능한 국제 표준 필요**
- **SPDX 3.0은 보안, 라이선스, AI, 데이터 세트 및 SW 패키징 구축 프로세스에 중점**
- **가장 인기있는 SBOM 생성 및 소비 사용 사례 해결을 위해 6가지 프로필 개발**
  - ➢SW가 기반이 되는 거의 모든 산업을 대표하는 광범위한 SPDX 커뮤니티 의견 기반으로 작성
  - ➢새로운 프로필은 SPDX가 글로벌 소프트웨어 공급망의 요구 사항을 충족하도록 보장
- **SPDX 3.0의 목표**
  - ➢SPDX 표준을 새로운 사용 사례로 확장하여 SW 엔지니어, 보안 전문가, 법률 및 규정 준수 전문가가 더 쉽게 사용하도록 하는 것
  - ➢SPDX 3.0은 SW 공급망 및 종속성 체인 투명성과 보안을 뒷받침하는 툴킷 역할을 함

SPDX 3.0 개발 현황

- **모델 설계를 위해 프로필을 병렬로 개발 중**
  - AI
  - Dataset
  - Core
  - Build
  - Licensing
  - Security
  - Software
- **SPDX 3.0 모델은 다소 시간이 소요될 것으로 예상됨**

토의

- **SBOM을 위해서 패키지 정보만으로 충분한가?**
  - ➢파일 정보와 Snippet 정보는 생략해도 무방
- **보안취약점 정보는 SBOM을 위한 필수 정보인가?**
  - ➢보안취약점 정보는 SPDX V2.3 Package information 부분의 external reference 필드 활용 가능 (2.1 버전부터 포함)
  - ➢필수 정보일지는 (상위) 지침에 기반될 것으로 예상
- **의존성 인과관계 포함 여부**
  - ➢의존성 인과관계 식별 후 SPDX 생성함으로써 표현 가능
  - ➢SPDX V2.3의 Relationship between SPDX Elements Information 파트에 기재
    - ✓ ‘DEPENDENCY_OF’
- **SW공급망을 위한 SBOM 생성에 SPDX, CycloneDX 모두 활용 가능**

감사합니다