OSS管理の重要性とSBOM活用

MACNICA

2022/7/7

株式会社マクニカ

イノベーション戦略事業本部

高畑　紀之

50th ANNIVERSARY

© Macnica, Inc.

アジェンダ

- 講演者について
- マクニカ概要
- SBOMについて
- SPDX解説

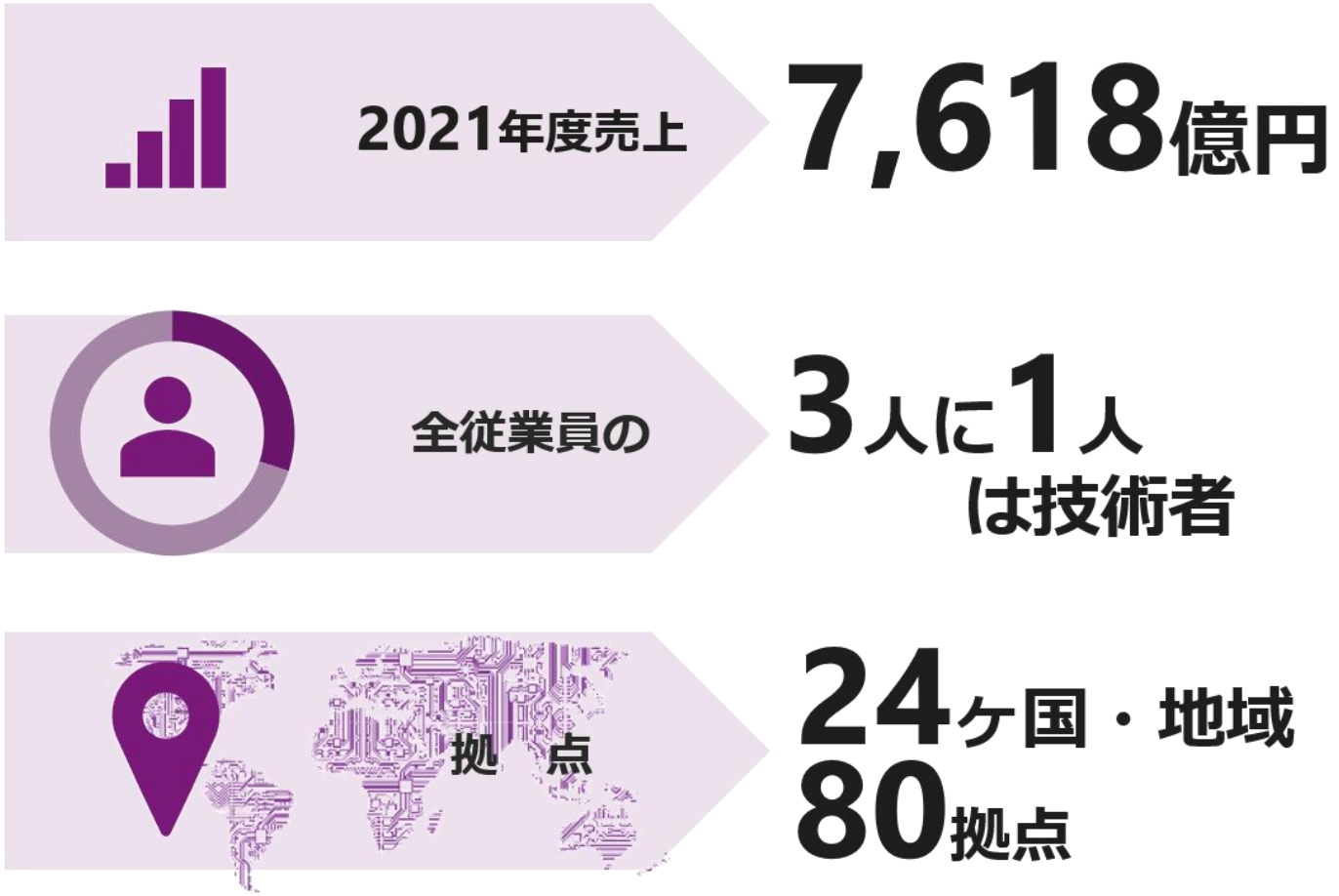
© Macnica, Inc.

講演者について

- 10年ほど鉄道向けの組み込みソフトウェア開発に従事
- 2019年マクニカ入社。入社以降、自動運転向けプラットフォームや車載カメラ等のFAEとして活動。
- 2021年よりBlackBerry社製品のFAEとして活動中。

© Macnica, Inc.

マクニカ概要



© Macnica, Inc.

“SBOM”
(ソフトウェア部品表)
を取り巻く環境

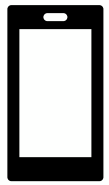
MACNICA

50th ANNIVERSARY

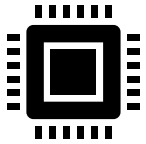
© Macnica, Inc.

BOM/SBOM

● BOM(Bill of Materials)
製品を構成する部品表

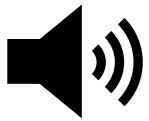


レンズ
イメージセンサー
画像処理プロセッサ

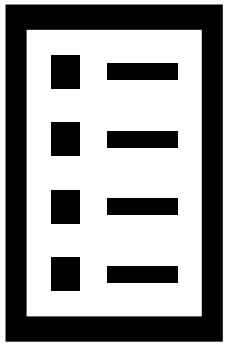


メインプロセッサ
Appプロセッサ
メモリー
通信用部品
スクリーン

バッテリー
バッテリ管理
非接触充電

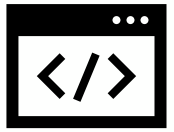


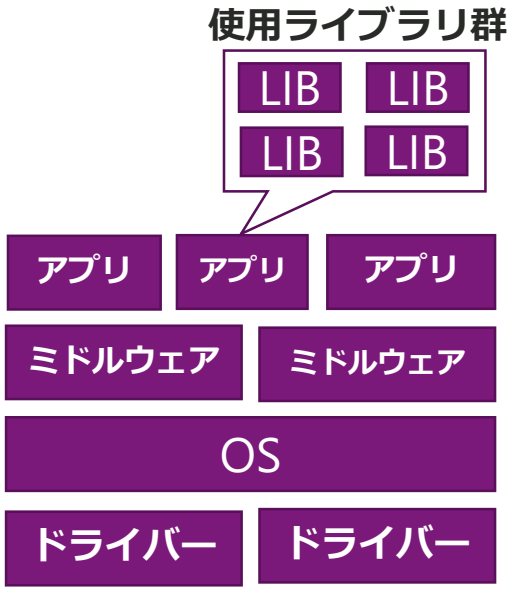
スピーカー
アンプ

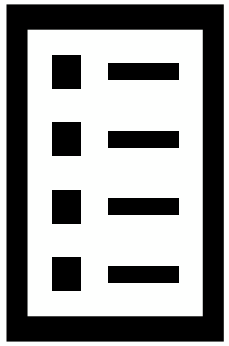


使用
コンポーネンツの
部品表

● SBOM(Software Bill of Materials)
製品を構成するソフトウェアの部品表







使用
ソフトウェアの
部品表

© Macnica, Inc.

SBOMが期待される背景

- **自動車業界**
  - 「ソフトウェアファースト」によるソフトウェアコード行数の増大
    - 約２億行に及ぶケースも(2020年)
    - ECU統合、仮想化技術などにより、ECUあたりのソフトウェア数が増大
  - コネクテッド機能によるアタックされる領域の拡大
    - トヨタ自動車では、サイバー攻撃の対策としてSBOMを活用

    出展：日経XTECH「トヨタが推すサイバー対策の新常識「SBOM」、流出するリスクは？
    https://xtech.nikkei.com/atcl/nxt/column/18/00001/06002/
  - WP29対応
- **医療機器分野**
  - 国際医療機器規制当局フォーラム（IMDRF)が医療機器のサイバーセキュリティ対策に関するガイダンスを発行
  - 日本でも医療機器の規制に取り入れ、2023年をめどに本格運用の方針

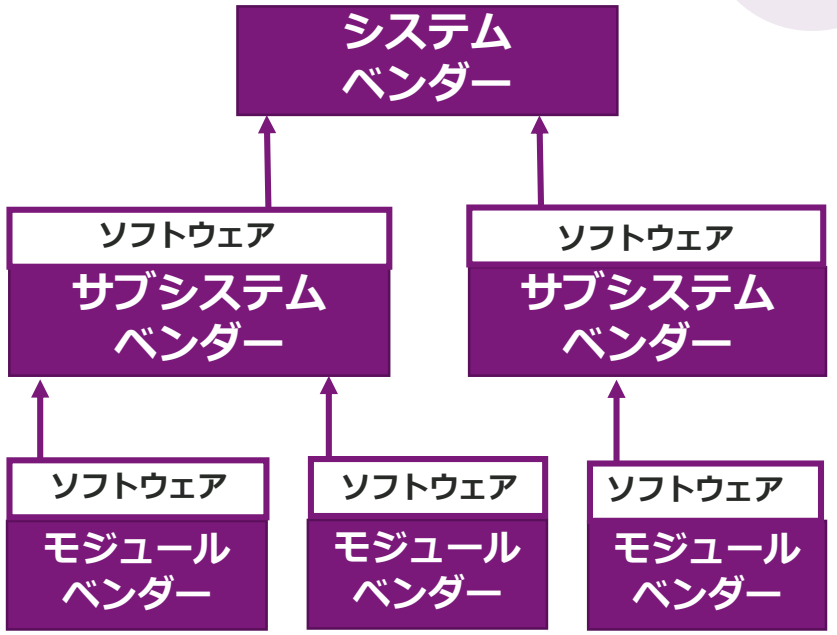
© Macnica, Inc.

システムベンダーの課題

- 複雑なサプライチェイン
- 提供元が異なる複数のソフトウェア
- ライセンス形態が異なるソフトウェアの混在
- 意図的・偶発的な脆弱性の内在

■サプライチェインのリスク
■ライセンスのコンプライアンス
　コピーレフト、準コピーレフト、
　非コピーレフト、GPL、BSD　など
■セキュリティや品質のリスク
　ソフトウェア脆弱性、配布プロセス

ソフトウェアのサプライチェイン

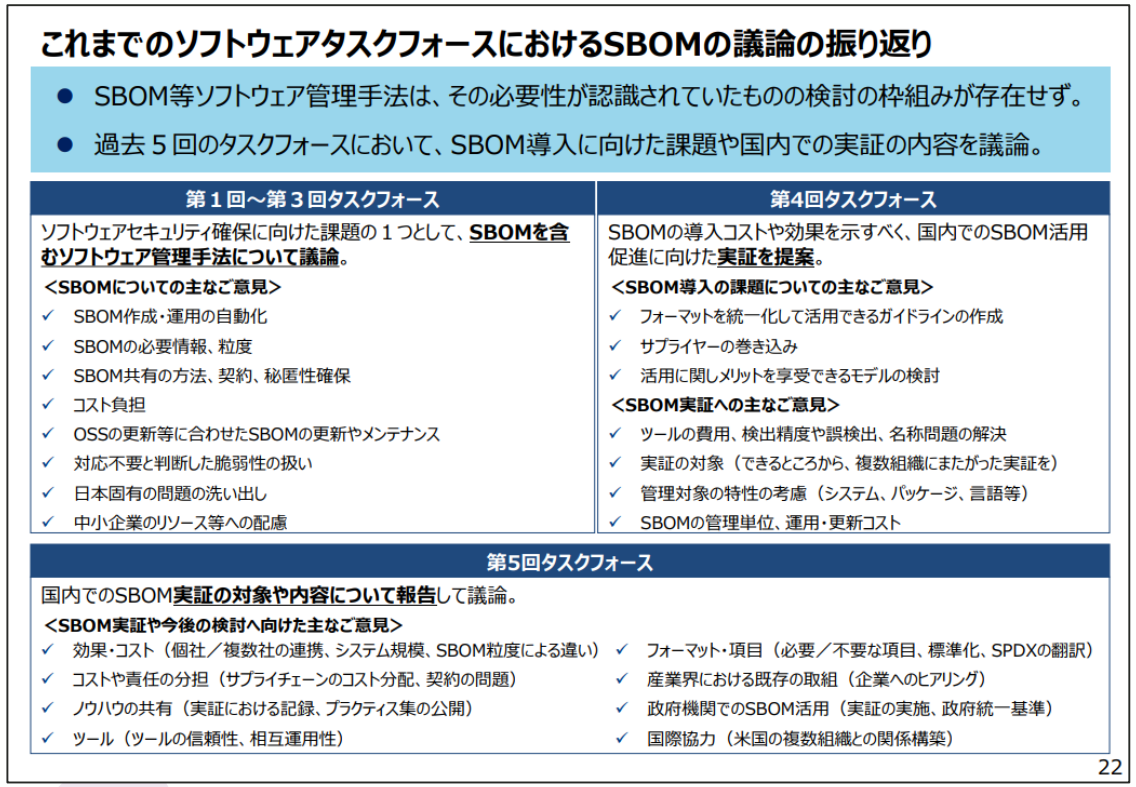


© Macnica, Inc.

SBOMの動向 -経済産業省-

- 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

- 産業サイバーセキュリティ研究会: ソフトウェア・システム開発ベンダが留意すべき事項として、「SBOMの提供」を挙げている



これまでのソフトウェアタスクフォースにおけるSBOMの議論の振り返り

- SBOM等ソフトウェア管理手法は、その必要性が認識されていたものの検討の枠組みが存在せず。
- 過去５回のタスクフォースにおいて、SBOM導入に向けた課題や国内での実証の内容を議論。

第１回～第３回タスクフォース

ソフトウェアセキュリティ確保に向けた課題の１つとして、**SBOMを含むソフトウェア管理手法について議論**。

<SBOMについての主なご意見>
- ✓ SBOM作成・運用の自動化
- ✓ SBOMの必要情報、粒度
- ✓ SBOM共有の方法、契約、秘匿性確保
- ✓ コスト負担
- ✓ OSSの更新等に合わせたSBOMの更新やメンテナンス
- ✓ 対応不要と判断した脆弱性の扱い
- ✓ 日本固有の問題の洗い出し
- ✓ 中小企業のリソース等への配慮

第4回タスクフォース

SBOMの導入コストや効果を示すべく、国内でのSBOM活用促進に向けた**実証を提案**。

<SBOM導入の課題についての主なご意見>
- ✓ フォーマットを統一化して活用できるガイドラインの作成
- ✓ サプライヤーの巻き込み
- ✓ 活用に関しメリットを享受できるモデルの検討

<SBOM実証への主なご意見>
- ✓ ツールの費用、検出精度や誤検出、名称問題の解決
- ✓ 実証の対象（できるところから、複数組織にまたがった実証を）
- ✓ 管理対象の特性の考慮（システム、パッケージ、言語等）
- ✓ SBOMの管理単位、運用・更新コスト

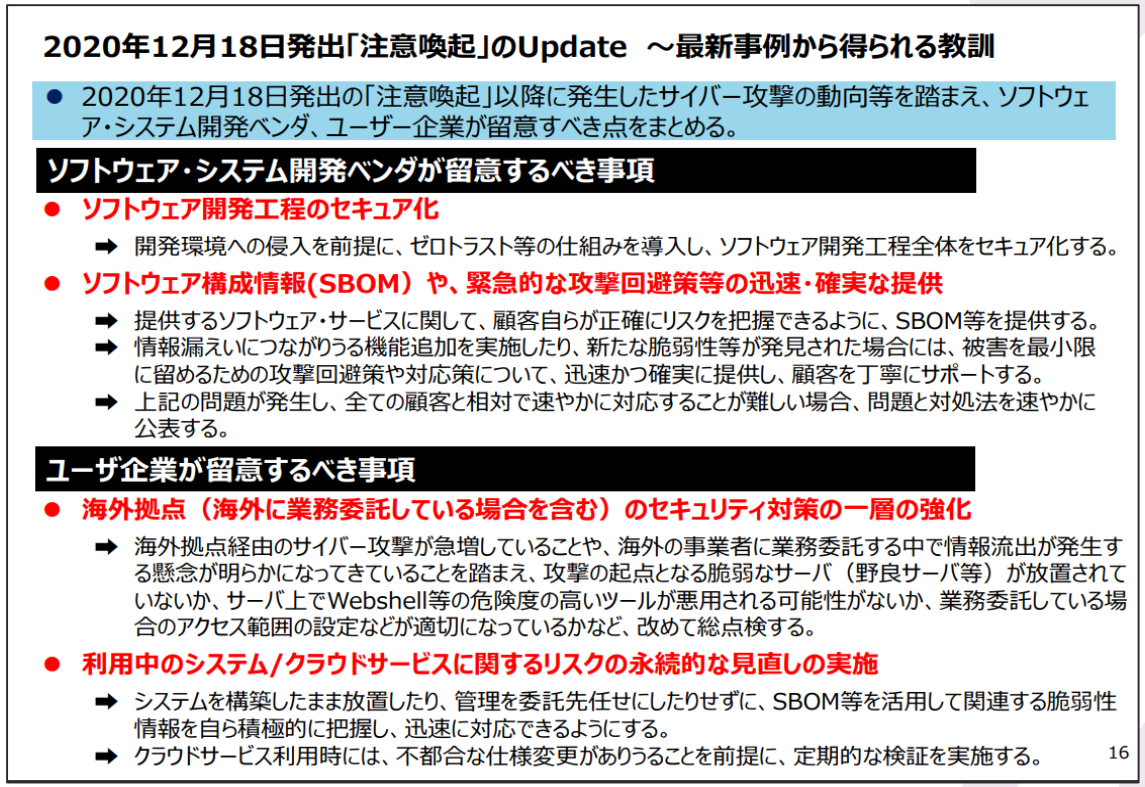
第5回タスクフォース

国内でのSBOM**実証の対象や内容について報告**して議論。

<SBOM実証や今後の検討へ向けた主なご意見>
- ✓ 効果・コスト（個社／複数社の連携、システム規模、SBOM粒度による違い）
- ✓ フォーマット・項目（必要／不要な項目、標準化、SPDXの翻訳）
- ✓ コストや責任の分担（サプライチェーンのコスト分配、契約の問題）
- ✓ 産業界における既存の取組（企業へのヒアリング）
- ✓ ノウハウの共有（実証における記録、プラクティス集の公開）
- ✓ 政府機関でのSBOM活用（実証の実施、政府統一基準）
- ✓ ツール（ツールの信頼性、相互運用性）
- ✓ 国際協力（米国の複数組織との関係構築）

22

出典：経済産業省「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/006_03_00.pdf



2020年12月18日発出「注意喚起」のUpdate ～最新事例から得られる教訓

- 2020年12月18日発出の「注意喚起」以降に発生したサイバー攻撃の動向等を踏まえ、ソフトウェア・システム開発ベンダ、ユーザー企業が留意すべき点をまとめる。

ソフトウェア・システム開発ベンダが留意するべき事項

- **ソフトウェア開発工程のセキュア化**
  - ➡ 開発環境への侵入を前提に、ゼロトラスト等の仕組みを導入し、ソフトウェア開発工程全体をセキュア化する。
- **ソフトウェア構成情報(SBOM）や、緊急的な攻撃回避策等の迅速・確実な提供**
  - ➡ 提供するソフトウェア・サービスに関して、顧客自らが正確にリスクを把握できるように、SBOM等を提供する。
  - ➡ 情報漏えいにつながりうる機能追加を実施したり、新たな脆弱性等が発見された場合には、被害を最小限に留めるための攻撃回避策や対応策について、迅速かつ確実に提供し、顧客を丁寧にサポートする。
  - ➡ 上記の問題が発生し、全ての顧客と相対で速やかに対応することが難しい場合、問題と対処法を速やかに公表する。

ユーザ企業が留意するべき事項

- **海外拠点（海外に業務委託している場合を含む）のセキュリティ対策の一層の強化**
  - ➡ 海外拠点経由のサイバー攻撃が急増していることや、海外の事業者に業務委託する中で情報流出が発生する懸念が明らかになってきていることを踏まえ、攻撃の起点となる脆弱なサーバ（野良サーバ等）が放置されていないか、サーバ上でWebshell等の危険度の高いツールが悪用される可能性がないか、業務委託している場合のアクセス範囲の設定などが適切になっているかなど、改めて総点検する。
- **利用中のシステム/クラウドサービスに関するリスクの永続的な見直しの実施**
  - ➡ システムを構築したまま放置したり、管理を委託先任せにしたりせずに、SBOM等を活用して関連する脆弱性情報を自ら積極的に把握し、迅速に対応できるようにする。
  - ➡ クラウドサービス利用時には、不都合な仕様変更がありうることを前提に、定期的な検証を実施する。

16

出典：経済産業省「第６回産業サイバーセキュリティ研究会事務局説明資料」
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/006_03_00.pdf

© Macnica, Inc.

SBOM活用の動向

		2022	2023	2024
日本	SBOM活用モデル、 取引モデル、 自動化・共有化の検討		実証の実施や施策の実施 →	
	国外との制度調和		取り組み案の実施	

- **SBOM活用の必要性**
  - ソフトウェアの構成比率が増加
    - ソフトウェア定義のプロダクト(SDV、SDN、SDx)
  - アジャイル開発での3rd Partyの活用
  - サイバーアタックの脅威の増大
  - ソフトウェアの様々なライセンス形態

品質の担保やリスクマネージメントのため、SBOMの重要性が向上

© Macnica, Inc.

SBOM作成に掛かるコスト

実証におけるコスト・効果に関する計測結果

- 実証により、工数・費用の項目を確認。今回の比較条件では、SBOMは導入のための初期工数（環境整備、学習等）が大きいが、運用工数（SBOM作成、活用）はツールの活用により従来の手作業部品管理に比べ小さい結果となり、**管理対象のソフトウェア部品が多いほど、SBOM導入効果が大きくなると想定**される。
- 脆弱性特定をツールで自動化することで、都度の確認にかかる工数を増やさず確認頻度を多く設定できるため、**脆弱性発表から特定までのリードタイムの短縮と工数の削減に繋がる**と考えられる。

シナリオ	初期工数		運用工数				ツール費用（初期・運用）
	環境整備工数	体制構築・学習工数	SBOM(部品情報)作成工数		脆弱性特定工数	ライセンス特定工数	
			作成工数	精査工数			
①従来の部品管理(独自形式)	1.3人時間 (フォーマットの定義)	0.5人時間 (フォーマット・運用の連携)	3.0分/部品	3.8分/部品 (OSS一覧のレビュー)	6分/部品・回 (頻度:1.5カ月)	10分/部品 *別途法務チェックに2-5営業日	(なし)
②SBOM(手動作成)	102.1人時間 (活用ツール導入・処理調査、テンプレート整備) *全社の合計値	48.2人時間 (SBOM作成方法の学習、作業手順書作成) *全社の合計値	2.9分/部品	(なし) *開発者が手動作成した部品情報が正確と仮定	0分/部品・回 (頻度:即時)	0分/部品 *別途法務チェックに2-5営業日 *ライセンスの検知漏れが発生	
③SBOM(無償ツール)	71.1人時間 (作成・活用ツール導入) *全社の合計値	57.2人時間 (作業手順書作成、学習) *全社の合計値	0.2分/部品	1.4分/部品 (検知結果確認)			
④SBOM(有償ツール)	3.0人時間 (商談、スキャン用アプリ導入)	6.5人時間 (学習、開発元問い合わせ)	0.3分/部品	1.4分/部品(検知結果確認) (81.5分/部品(OSSの依存関係の解析によって新たに検知した部品に関する精査及びベンダー確認))	0分/部品・回 (頻度:即時)	0分/部品 *別途法務チェックに2-5営業日	ユーザー数やデータ量等に応じたライセンス費用が発生

- **管理するソフトウェア部品数が多い場合や脆弱性特定頻度が高い場合等、各シナリオにおいて網掛けした工数が支配的**となる。
- 本実証における部品件数は7件（Pythonのrequirement.txtにより規定されるOSS部品の粒度）。有償ツールでは追加で再利用部品11件を検知。
- **本実証では、工数測定にあたって各ツールの検出精度や対象ソフトウェアの特性は考慮していない。実際に導入を検討する際は、工数だけではなく精度についても検討・評価が必要であり、本事例の計測値をもって直接的にSBOMの有効性を一般化して主張するものではない点に留意。**

29

出典：経済産業省「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/006_03_00.pdf

© Macnica, Inc.

“BlackBerry Jarvis 2.0” の有用性

MACNICA

50th ANNIVERSARY

© Macnica, Inc.

BlackBerry Jarvis 2.0 の特徴

- 政府系で採用されているセキュリティアルゴリズム
- 高速・高性能のスキャニングエンジン
- 直観的なユーザインターフェイス
- CVE更新等の通知機能と潜在的な脆弱性の検知
- 国際規格のSPDX、CycloneDXフォーマットの対応

ワンクリックで潜在的なセキュリティ問題を特定

© Macnica, Inc.

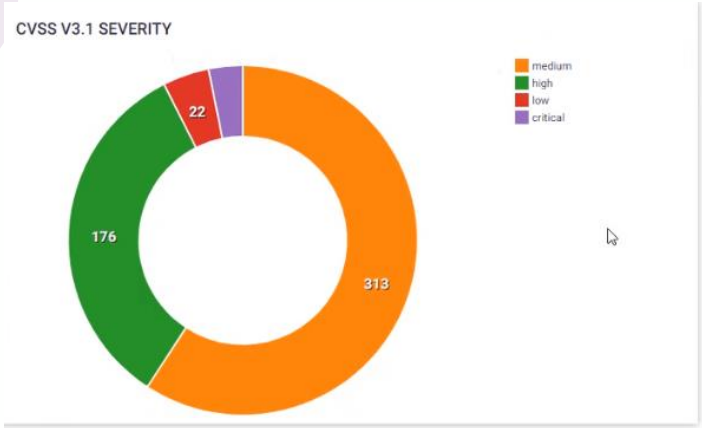
組み込みシステムに最適なツール

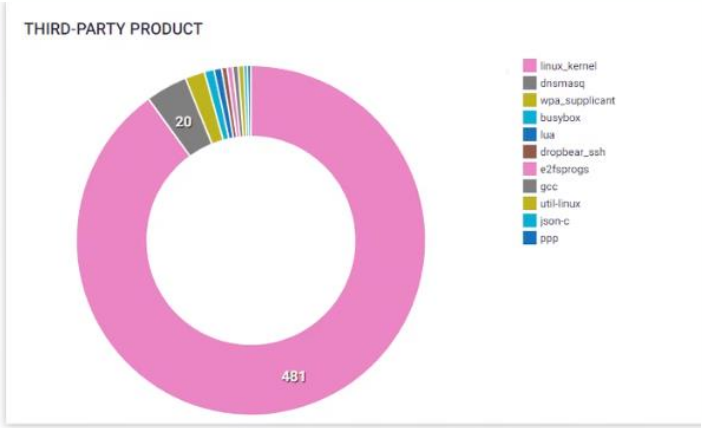
様々なファイルフォーマットやアーキテクチャをサポート

アーカイブ形式	ハードウェア	対応OS	対応言語
・各種圧縮形式 ZIP,GZIP,TAR,RAR,AR etc ・仮想マシンのバイナリ形式 VMDK,QCOW2, DOSパーティションズ ・Linux/Unixパッケージファイル形式 ・Androidパッケージファイル形式 ・各種ファイルシステムのアーカイブ	ARM Intel x86 Power 32 bit, VLE ルネサス V850,RH850 etc. インフィニオン TriCore MIPS 32 bit Sparc 32 bit AVR 32	Linux：ELF ,SO Android：ELF , SO, APK QNX 6/7：ELF, SO VxWorks 5/6 Classic AutoSAR Dalvik：ART Oracle Java: Jar, Class Media：EXIF, geo tag etc	C C++ Java Assembly

© Macnica, Inc.

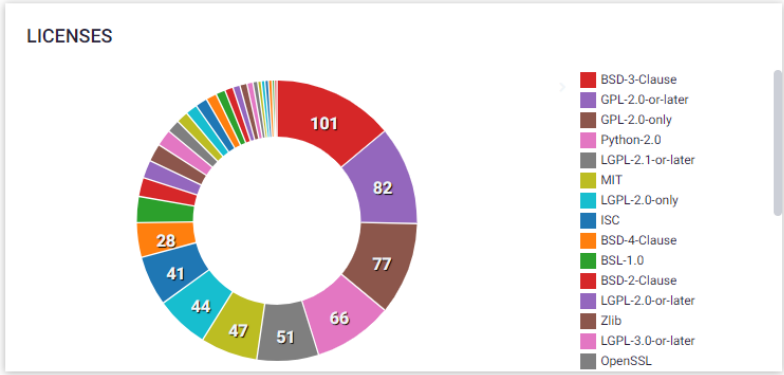
Jarvis 2.0 画面イメージ

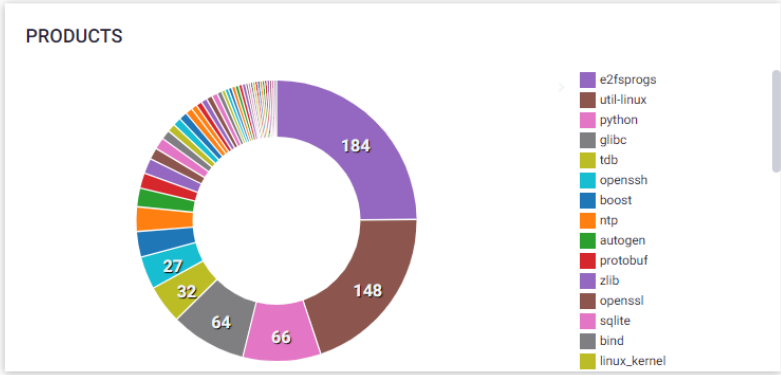




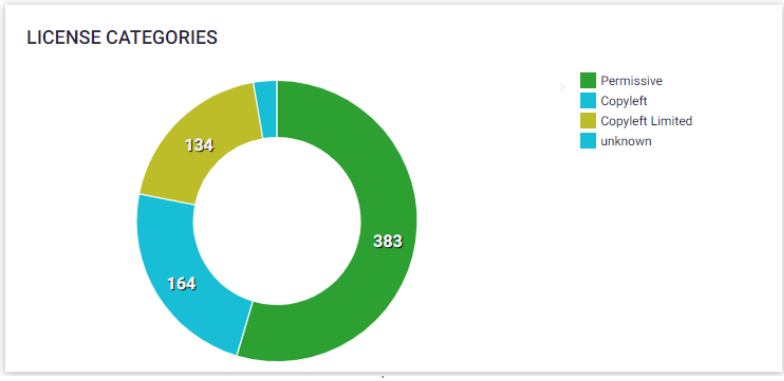
←CVE診断結果一覧

CVE » NAME	PRODUCT	PRODUCT VERSION	FIXED IN	CVE » CVSS » V31 » BASE SEVERITY	CVE » CVSS » V31 » BASE SCORE
CVE-2019-18805	linux_kernel	4.14.95	[4.14.115, 4.19), [4.19.38, 5.0), [5.0.11, 5.1), > 5.1	critical	9.8
CVE-2018-12714	linux_kernel	4.14.95	> 4.17.2	critical	
CVE-2019-18814	linux_kernel	4.14.95	> 5.3.9	critical	
CVE-2019-15504	linux_kernel	4.14.95	> 5.2.9	critical	
CVE-2019-17133	linux_kernel	4.14.95	> 5.3.2	critical	
CVE-2017-14493	dnsmasq	2.73	> 2.77	critical	
CVE-2018-1000517	busybox	1.28.4	>= 1.29.0	critical	
CVE-2019-15505	linux_kernel	4.14.95	> 5.2.9	critical	
CVE-2019-15292	linux_kernel	4.14.95	>= 5.0.9	critical	





ライセンス一覧→



SPDXフォーマットについて

- Software Package Data Exchangeの略
- Linux foundationが仕様策定
- 2021年9月、ISO/IEC 5962:2021 として公開され、国際オープン標準として認められた
- ソフトウェアパッケージに関する情報(パッケージ名、ライセンス、バージョン等)を統一フォーマットで記載することで、組織間のやりとりをスムーズに行えるようにしたもの ⇒ **SBOMのフォーマットとして使える！**

© Macnica, Inc.

SBOMの要素とSPDXの対応

- 先行しているアメリカでは、SBOMに記載すべき最小要素について下表のように定義
- 業界によっては最小要素以外の項目(checksum field等)も必須とする動きがある
- SPDX 2.2ではこれらの要素をカバーできるようになっている

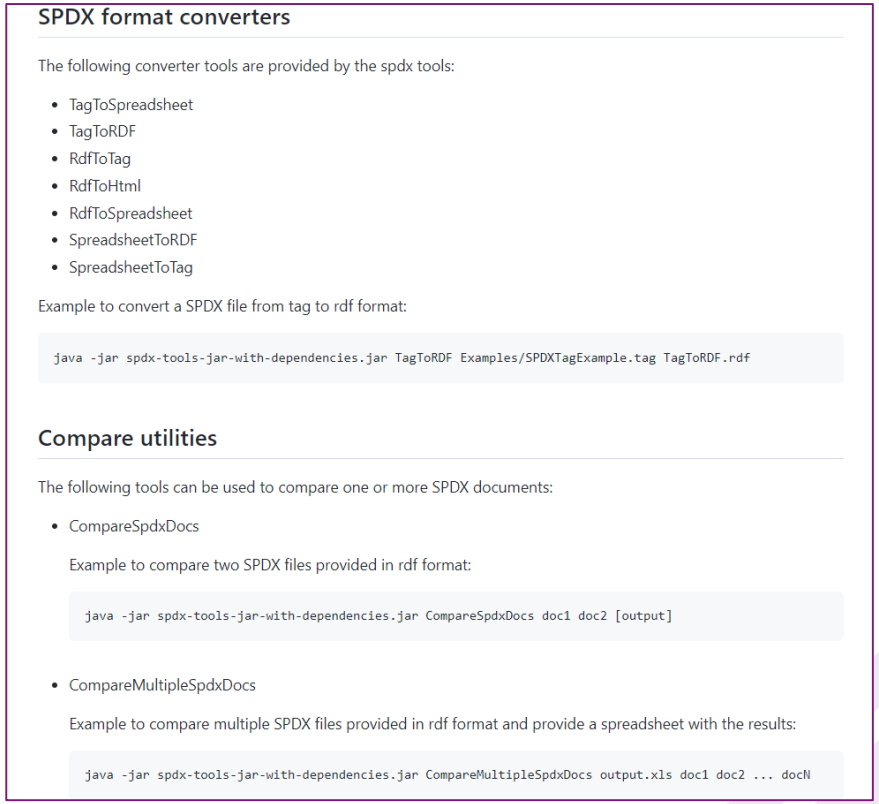
表 SBOM最小要素

カテゴリ	定義
Data Fields データフィールド	必要な各コンポーネントに関するベースライン情報を文書化すること ・サプライヤー名 ・コンポーネント名 ・コンポーネントバージョン ・その他のユニーク識別子 ・依存関係 ・SBOM作成者 ・タイムスタンプ
Automation Support 自動化サポート	SBOMの自動生成や可読性などの自動化をサポートすること
Practices and Processes 運用方法	SBOMの要求、生成、利用に関する運用方法を 定義すること

© Macnica, Inc.

SPDXファイル関連ツール

- SPDX.orgにてSPDX関連ツールが公開(https://spdx.dev/resources/tools/)
- Python版やJava版、JavaScript版等が用意されている
- Tag、RDF、XLSなど様々なファイルフォーマットに変換可能
- SPDXファイル同士の比較も行える



SPDX format converters

The following converter tools are provided by the spdx tools:

- TagToSpreadsheet
- TagToRDF
- RdfToTag
- RdfToHtml
- RdfToSpreadsheet
- SpreadsheetToRDF
- SpreadsheetToTag

Example to convert a SPDX file from tag to rdf format:

```
java -jar spdx-tools-jar-with-dependencies.jar TagToRDF Examples/SPDXTagExample.tag TagToRDF.rdf
```

Compare utilities

The following tools can be used to compare one or more SPDX documents:

- CompareSpdxDocs

  Example to compare two SPDX files provided in rdf format:

  ```
  java -jar spdx-tools-jar-with-dependencies.jar CompareSpdxDocs doc1 doc2 [output]
  ```

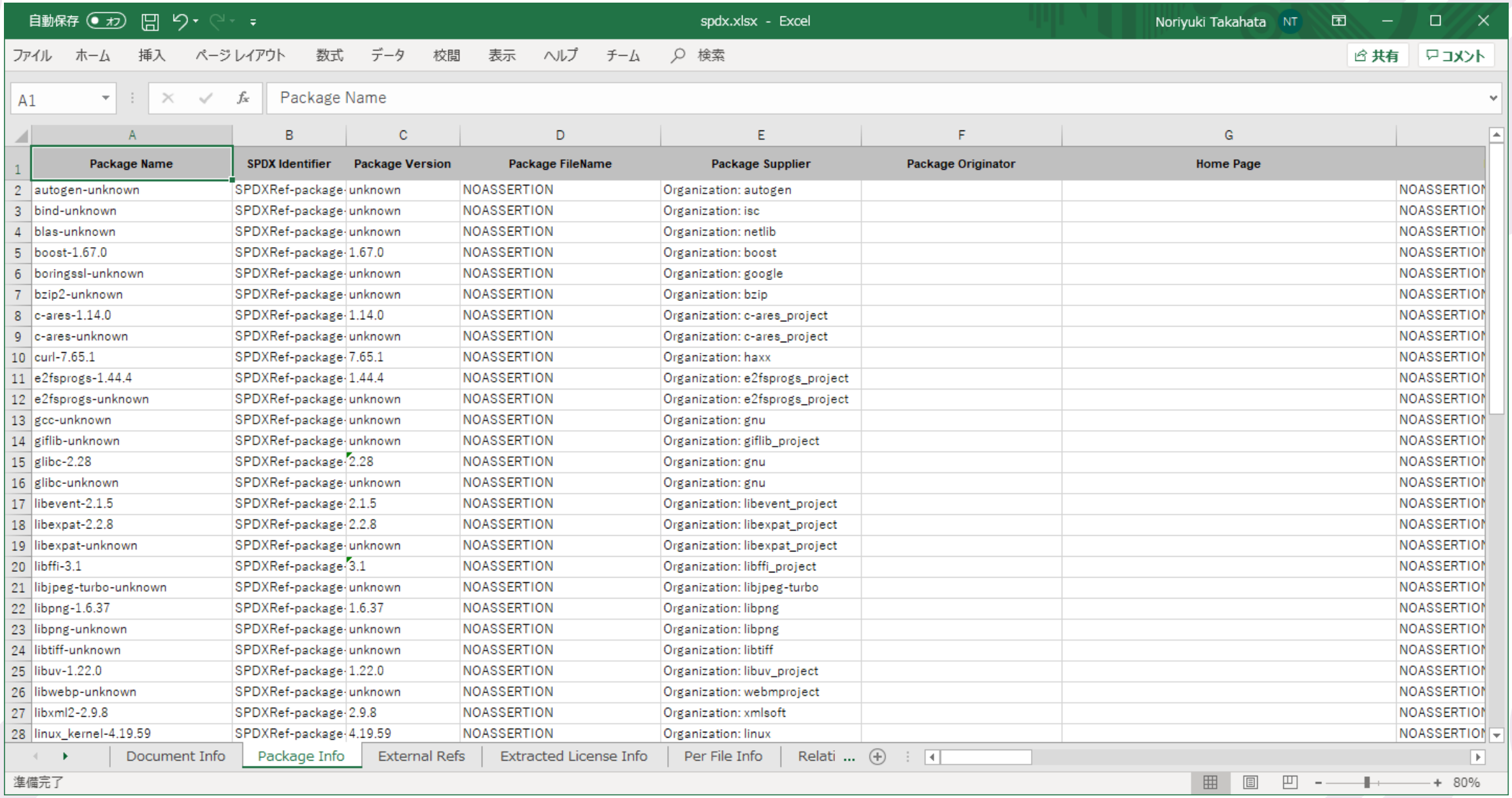
- CompareMultipleSpdxDocs

  Example to compare multiple SPDX files provided in rdf format and provide a spreadsheet with the results:

  ```
  java -jar spdx-tools-jar-with-dependencies.jar CompareMultipleSpdxDocs output.xls doc1 doc2 ... docN
  ```

© Macnica, Inc.

SPDXフォーマットの出力例(XLS形式に変換)



	A	B	C	D	E	F	G	
1	Package Name	SPDX Identifier	Package Version	Package FileName	Package Supplier	Package Originator	Home Page	
2	autogen-unknown	SPDXRef-package-	unknown	NOASSERTION	Organization: autogen			NOASSERTION
3	bind-unknown	SPDXRef-package-	unknown	NOASSERTION	Organization: isc			NOASSERTION
4	blas-unknown	SPDXRef-package-	unknown	NOASSERTION	Organization: netlib			NOASSERTION
5	boost-1.67.0	SPDXRef-package-	1.67.0	NOASSERTION	Organization: boost			NOASSERTION
6	boringssl-unknown	SPDXRef-package-	unknown	NOASSERTION	Organization: google			NOASSERTION
7	bzip2-unknown	SPDXRef-package-	unknown	NOASSERTION	Organization: bzip			NOASSERTION
8	c-ares-1.14.0	SPDXRef-package-	1.14.0	NOASSERTION	Organization: c-ares_project			NOASSERTION
9	c-ares-unknown	SPDXRef-package-	unknown	NOASSERTION	Organization: c-ares_project			NOASSERTION
10	curl-7.65.1	SPDXRef-package-	7.65.1	NOASSERTION	Organization: haxx			NOASSERTION
11	e2fsprogs-1.44.4	SPDXRef-package-	1.44.4	NOASSERTION	Organization: e2fsprogs_project			NOASSERTION
12	e2fsprogs-unknown	SPDXRef-package-	unknown	NOASSERTION	Organization: e2fsprogs_project			NOASSERTION
13	gcc-unknown	SPDXRef-package-	unknown	NOASSERTION	Organization: gnu			NOASSERTION
14	giflib-unknown	SPDXRef-package-	unknown	NOASSERTION	Organization: giflib_project			NOASSERTION
15	glibc-2.28	SPDXRef-package-	2.28	NOASSERTION	Organization: gnu			NOASSERTION
16	glibc-unknown	SPDXRef-package-	unknown	NOASSERTION	Organization: gnu			NOASSERTION
17	libevent-2.1.5	SPDXRef-package-	2.1.5	NOASSERTION	Organization: libevent_project			NOASSERTION
18	libexpat-2.2.8	SPDXRef-package-	2.2.8	NOASSERTION	Organization: libexpat_project			NOASSERTION
19	libexpat-unknown	SPDXRef-package-	unknown	NOASSERTION	Organization: libexpat_project			NOASSERTION
20	libffi-3.1	SPDXRef-package-	3.1	NOASSERTION	Organization: libffi_project			NOASSERTION
21	libjpeg-turbo-unknown	SPDXRef-package-	unknown	NOASSERTION	Organization: libjpeg-turbo			NOASSERTION
22	libpng-1.6.37	SPDXRef-package-	1.6.37	NOASSERTION	Organization: libpng			NOASSERTION
23	libpng-unknown	SPDXRef-package-	unknown	NOASSERTION	Organization: libpng			NOASSERTION
24	libtiff-unknown	SPDXRef-package-	unknown	NOASSERTION	Organization: libtiff			NOASSERTION
25	libuv-1.22.0	SPDXRef-package-	1.22.0	NOASSERTION	Organization: libuv_project			NOASSERTION
26	libwebp-unknown	SPDXRef-package-	unknown	NOASSERTION	Organization: webmproject			NOASSERTION
27	libxml2-2.9.8	SPDXRef-package-	2.9.8	NOASSERTION	Organization: xmlsoft			NOASSERTION
28	linux_kernel-4.19.59	SPDXRef-package-	4.19.59	NOASSERTION	Organization: linux			NOASSERTION

© Macnica, Inc.

SPDXの具体例(1)

Document Info

項目	例
SPDXバージョン	SPDX-2.2
ドキュメント名	Sample
SBOM作成者	Tool: BlackBerry Jarvis 0.1.930 Person: takahata
タイムスタンプ	2022/6/16 15:59:30
チェックサム	MD5: b92ac62e1c062e0bc78418a28fda9d56 SHA1: c60b4ef3915ee413a42f133d08e5f3496b10390b SHA256: a23654f3b077aa0cfdce702a08a5203a254bd9d8a9de6202f281b5f20b69ce26 SHA512: 943978837952bd6bda79847723b375a1d7ef04df311dd5225a22f0ef2351e8c3b34575135d965663f77ae290f664dc997e402ce6317a29031ac8ebaa1037d0e7

© Macnica, Inc.

SPDXの具体例(2)

Package Info

項目	例
サプライヤー名	Organization: busybox
コンポーネント名	busybox
コンポーネントバージョン	1.28.4-2
識別子	SPDXRef-package-busybox-da2e2bd5-b745-4496-a24e-d433c0d77f3e

Per File Info

項目	例
ファイル名	/Sample-x86.img.gz/image.raw/partition.2/bin/busybox
ファイルタイプ	BINARY
ライセンス情報	GPL-2.0-only
依存関係	CONTAINED_BY SPDXRef-package-busybox-da2e2bd5-b745-4496-a24e-d433c0d77f3e DYNAMIC_LINK SPDXRef-file-libc.so-f98e2633-95e3-4b92-9bdb-68917bf4e22f DYNAMIC_LINK SPDXRef-file-libgccs.so.1-597672c3-d27d-416b-9450-04aaf63dd6fb

© Macnica, Inc.

サマリー

- 国内外でSBOMに関する検討が活発
- SBOM作成ツール(BlackBerry Jarvis 2.0)の紹介
- SPDXフォーマットで記載されたSBOMの内容について紹介

SBOMが求められる時代はすぐそこ！
ツールを有効活用し、クリエイティブ活動にフォーカス！

経済産業省
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/006_03_00.pdf

経済産業省
最近の産業サイバーセキュリティに関する動向について
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_uchu_sangyo/pdf/003_03_00.pdf

© Macnica, Inc.

BlackBerry Jarvis 2.0評価ライセンス

- 30日間の無償評価ライセンス発行可能です。
  https://blackberry.qnx.com/en/products/security/blackberry-jarvis

デモブースにて、Jarvis 2.0 のデモを実施しています。
ぜひお立ち寄りください。

© Macnica, Inc.

Co.Tomorrowing

- 本資料に記載されている会社名、商品またはサービス名等は各社の商標または登録商標です。なお、本資料中では、「™」、「®」は明記しておりません。
- 本資料のすべての著作権は、第三者または株式会社マクニカに属しており、（著作権法で許諾される範囲を超えて）無断で本資料の全部または一部を複製・転用等することを禁じます。
- 本資料は作成日現在における情報を元に作成されておりますが、その正確性、完全性を保証するものではありません。

© Macnica, Inc.