



# トヨタのOSPO活動について



## TOYOTA Open Source

トヨタ自動車株式会社  
先進技術開発カンパニー  
オープンソースプログラムグループ付  
グループ長  
遠藤 雅人

貢献

2021  
HSR Simulator  
コード公開



2020  
Cloud Native Computing Foundation(CNCF)参加

2012  
Automotive Grade Linux(AGL)設立

2017  
OpenChain Project参加

2011  
Linux Foundation参加

2016  
Open Invention Network (OIN)出資

利活用

[https://www.toyota-tokyo.tech/news/pdf/240830report\\_ja.pdf](https://www.toyota-tokyo.tech/news/pdf/240830report_ja.pdf)

# トヨタのこれまでのOpenChainへの取り組み



2020  
AGLとコラボして  
CES出展

2021  
SPDX Liteが  
ISO/IEC 5962:2021の一部に

2020 ISO/IEC5230(OpenChain)  
認証取得(世界初の公表)

2019  
Automotive WGを設立(業界別初)

2018  
名古屋オフィスにてJP WGの  
全体会合をホスト

2017/12  
ソニー/日立とJapan WG設立(国別初)

2017/8  
Open Chainに  
プラチナメンバーとして参画(日本初)

[https://www.toyota-tokyo.tech/news/pdf/240830report\\_ja.pdf](https://www.toyota-tokyo.tech/news/pdf/240830report_ja.pdf)



# OSPOについて

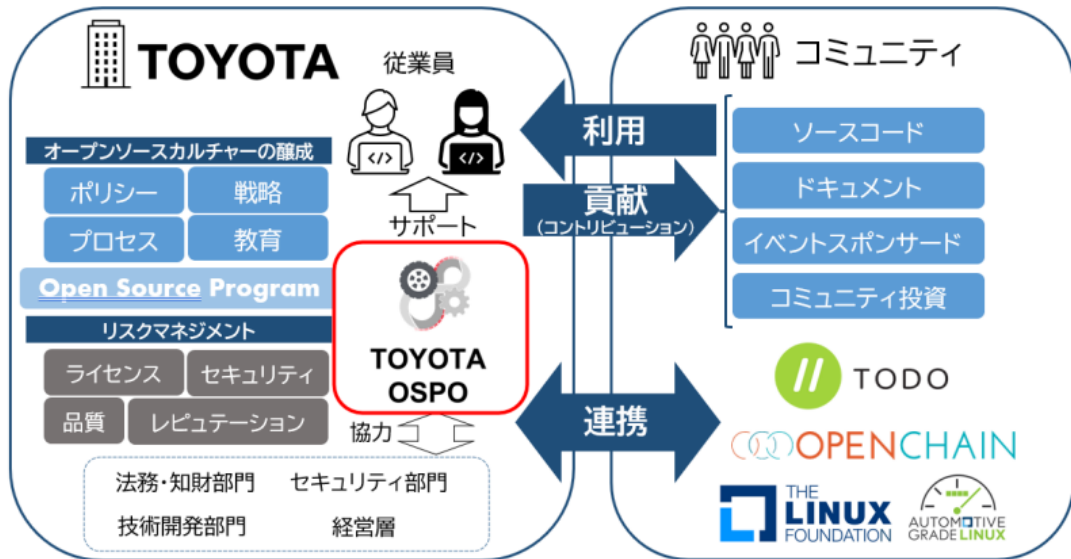
---



## **TOYOTA Open Source**

## OSPO(Open Source Program Office)とは？

OSSの「**貢献**」と「**利用**」を推進し、これらの活動を従業員が安心して行うことができるよう、ルールやプロセスを含めた体制整備・運用を行う**社内組織**



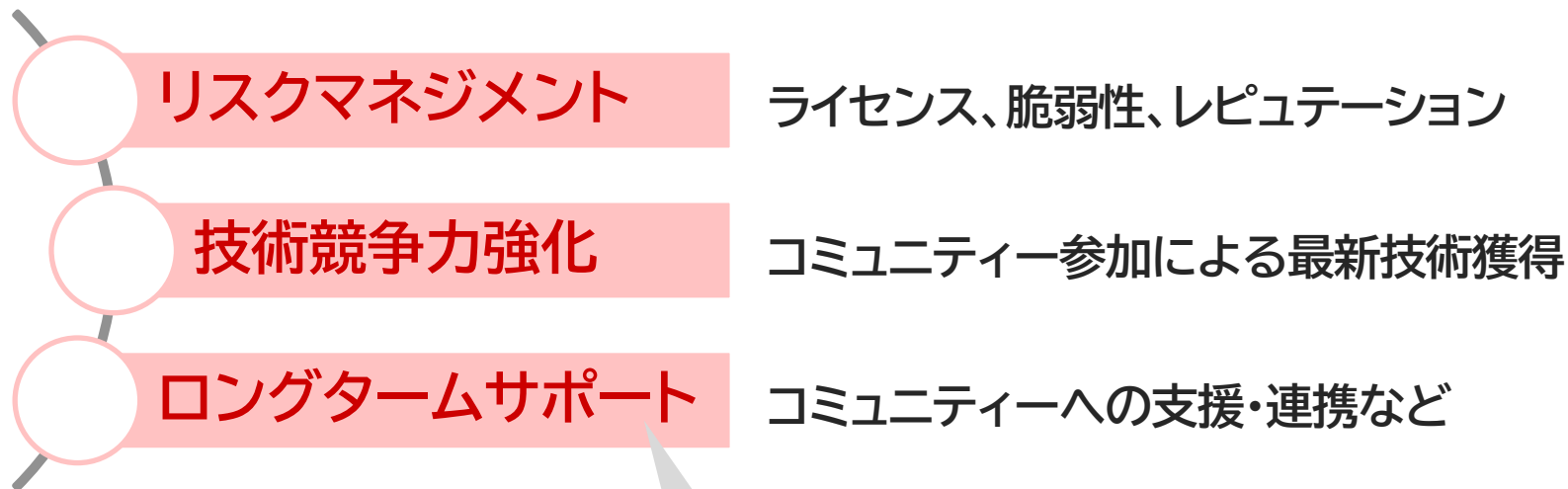
大手町の若手がボランティアに参加



大手町には世界中のコミュニティの皆様が訪れる

## なぜOSPOが必要？

弊社では、下記の強化のために組織化が必要と考えました

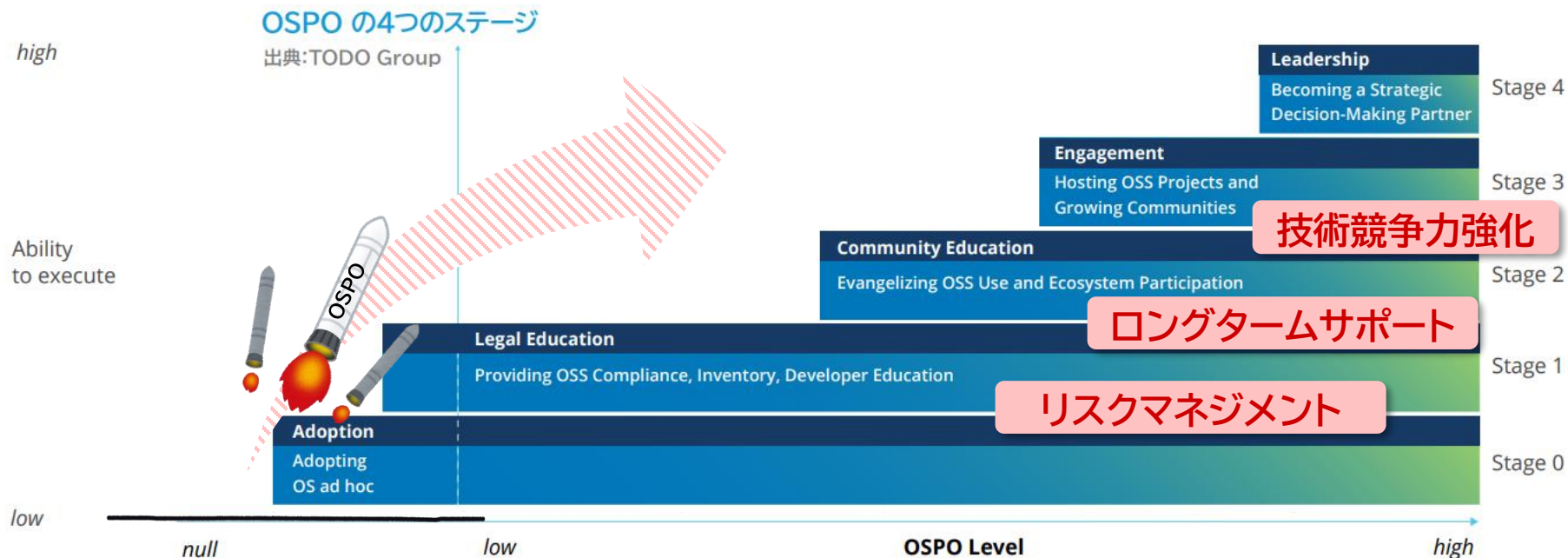


セキュリティリスクで申し上げましたLog4J問題ですが  
GitHubでLog4jのメンテナーが3名だったという

## どこを目指すのか？

活動するには目標が必要ですよね

強化したいテーマをマッピングすると下記ようになります



## ■ 弊社の具体的な取り組みに当てはめると…

### 1. 社員参加のコミュニティ活動への支援

技術競争力強化

ロングタームサポート



...

取り組み紹介①

取り組み紹介④

### 2. OSPOとしてのコミュニティ連携活動

技術競争力強化

リスクマネジメント



...

取り組み紹介③

取り組み紹介②



## 取り組み紹介① eBPF Japan初イベント開催

CNCFの日本支部である CNCJ の SIG として  
eBPF Japan Community が2024年に運営開始。

弊社OSPOであり、CNCJオーガナイザでもある多田が  
初イベントとして8月に **eBPF Japan Meetup** 開催  
異業種間でeBPFの情報交換が活発に行われた。



K8sなど多くのクラウド技術に関する  
OSSプロジェクトを持つ財団

- ※ CNCF : Cloud Native Computing Foundation
- ※ CNCJ : Cloud Native Computing Japan
- ※ SIG : Special Interest Group
- ※ eBPF : extended Berkeley Packet Filter



トヨタ大手町で登壇する  
OSPOの多田 健太 主幹

## 取り組み紹介② OSPO-EGの立ち上げ

自動車業界のエンジニアのOSSコミュニティ活動  
活性化のため、24年7月にドイツで開催された  
AGL AMM 2024にて、弊社OSPOの伊藤が  
**OSPO-EG(Expert Group)設置**を提案。

提案は承認され、OSPOの設置推進・OSPO間の情報・  
ベストプラクティスの共有を行うための場として、  
今後活動を本格化。  
企業のエグゼクティブ資料やOSPOのショーケース  
収集などを実施中。

※ AGL : Automotive Grade Linux

※ AMM : All-Member-Meeting



AGL AMM 2024で提案する  
OSPOの伊藤 雅典 主査

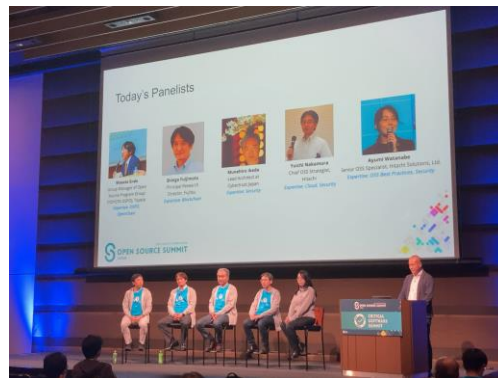
## 取り組み紹介③ Japan Evangelist Programへの参画 弊社の遠藤が「初代 Japan Evangelist」に就任



Japan Evangelistは、地域のコミュニティリーダーとして  
日本から世界的なイノベーション推進の場で活躍する機会を経験や情報でサポート  
地域に根ざした固有の文化や言語に対応したコミュニティ活動を推進



弊社OSPOリーダー  
遠藤 雅人(Masato Endo)



OSSJ2024における  
パネルディスカッションの様様

## 取り組み紹介④ Rustへの取り組み

Safety-Critical Rust Consortiumに参画し、  
Rustのツールチェーン開発を進めるWoven by TOYOTA  
と連携して、Rust言語の自動車業界における普及を目指す



Rust活動のキーパーソン  
JF Bastien



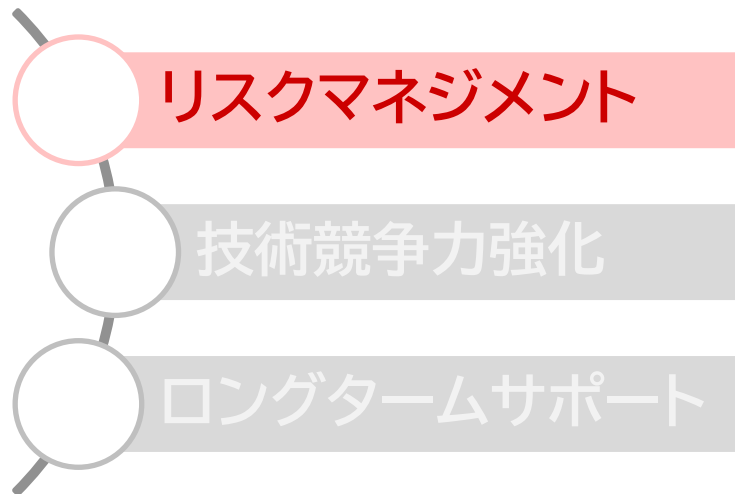
# SBOMとサプライチェーン

---



**TOYOTA Open Source**

(OSPOで強化する取り組み)



ライセンス、脆弱性、レピュテーション

コミュニティ参加による最新技術獲得

コミュニティへの支援・連携など

## OSS活用ステップ

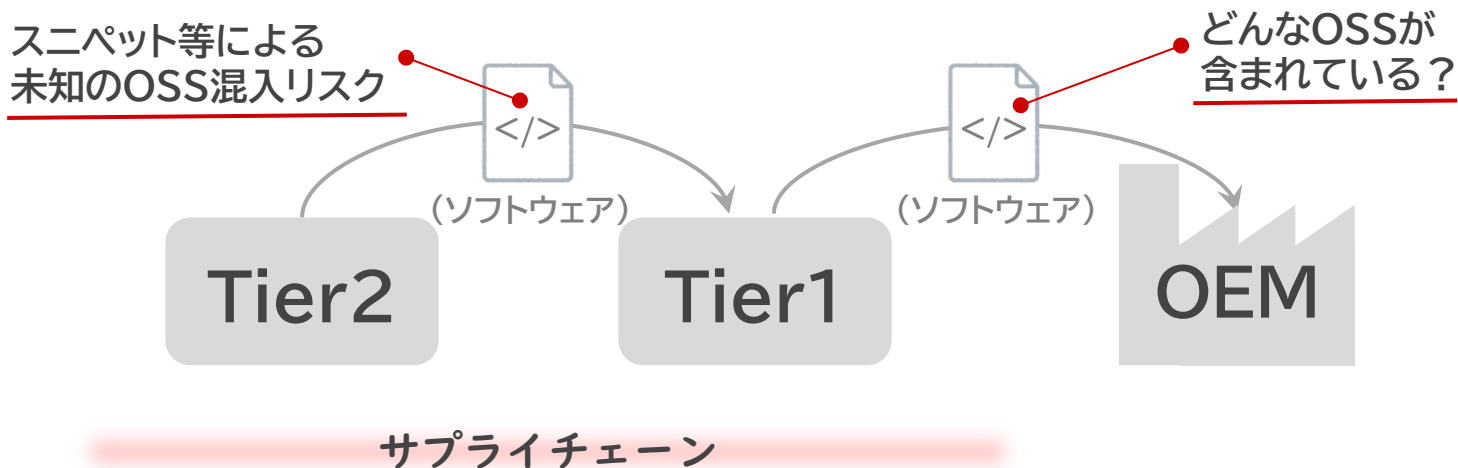
### 開発製品にOSSを活用する流れ



## サプライチェーン(SC)におけるOSSリスク

- ・ 製品にどのようなOSSが含まれているかわからない
- ・ OSSが紛れ込み、未知のリスクに直面する可能性

→ OSSがわかったとしても**問題があった場合**、製品リリースが遅れる

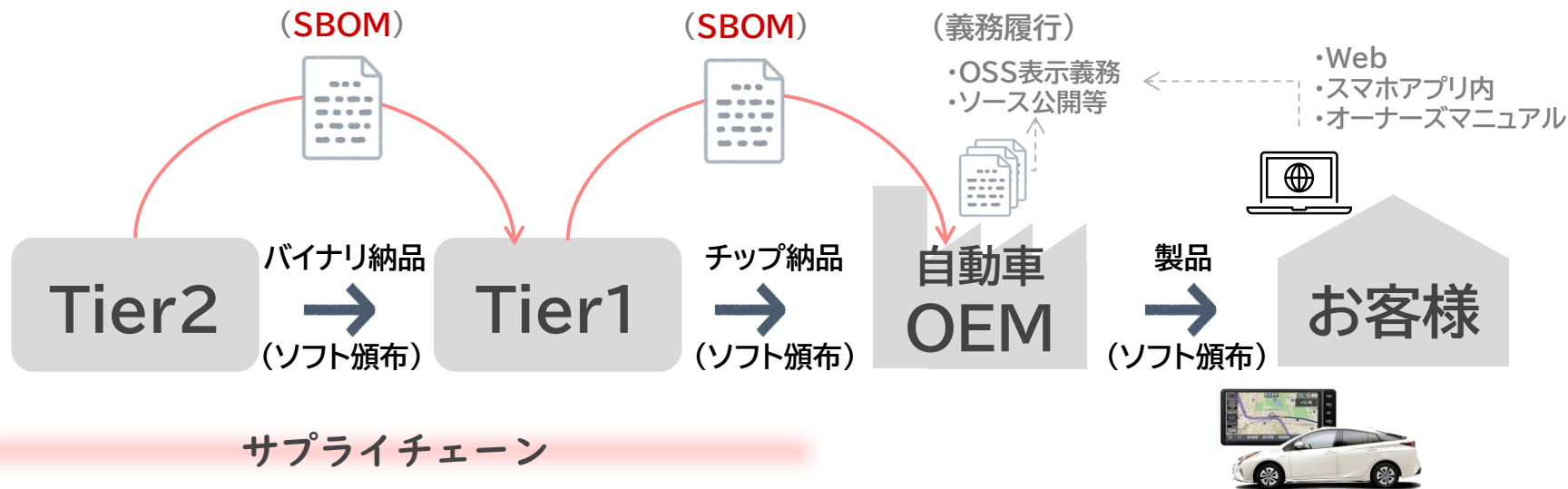




## 自動車業界におけるSBOM共有の重要性


チップやバイナリで納品される場合には、ソフトウェアの**中身がわからない場合有**

→ **ソースコードが入手できない場合は SBOMを確実に共有** する事が重要



## SBOM(Software Bill of Material)とは 「ソフトウェア部品表 のこと」

### SBOM(ソフトウェア部品表)




搭載S/W

製品	使用OSS (Ver)
ナビ	OpenSSL (1.1.1b), icu(60.2), sqlite(3.20.0), cairo(1.14.10), .....
DCM	.....
...	.....

(イメージ)

=



の原材料は？

名称	チョコレート
原材料名	砂糖、カカオマス全粉乳、ココアバター、植物油、でん粉、水あめ、ゼラチン、卵殻カルシウム、乳化剤、増粘剤(アラビアガム)、着色料(フラボノイド、クチナシ、カロチノイド、ビートレッド、スピルリナ青、イカ墨)、香料、光沢剤、セルロース、(一部に卵・乳成分・いか・大豆・ゼラチンを含む)
内容量	32g
賞味期限	右部に記載
保存方法	28℃以下の涼しい場所で保存してください。
製造者	〇〇〇株式会社
製造所	〇〇県〇〇市〇〇〇〇〇

(食品表示法で義務化)

SBOMは、ソフトウェアに含まれる  
OSS部品(コンポーネント)を**可視化**する



### SBOMへの関心が高まる

2021年5月12日の米国大統領令には  
政府調達ソフトウェアとして  
**ソフトウェア・サプライチェーン・セキュリティ**  
強化の項目でSBOM管理が盛り込まれた

デジタルインフラの **透明性**



脆弱性管理やライセンス遵守活動を円滑  
に行うためのツール、それが **SBOM**

## そのSBOMには何を書くのか？

### 使用しているOSSの素性を書く

項目	具体例
OSS名称	zlib
バージョン	1.2.3
入手先	<a href="https://zlib.net/fossils/zlib-1.2.3.tar.gz">https://zlib.net/fossils/zlib-1.2.3.tar.gz</a>
提供元	zlib
OSSライセンス	Zlib
...	...

使用しているOSS分



まとめる



一つひとつOSSの素性を列挙、まとめるとSBOMが出来上がる  
ただ、書き方や項目に統一性がないと情報交換できない  
→ そこで **SBOMフォーマット** の登場

## SBOMの書き方: SBOMフォーマット

SBOMのグローバル標準は **SPDX/SWID tag/CycloneDX** の3種類  
米バイデン政権の大統領令においても何れかでの提出が求められている

	フォーマット	策定主体	特徴
1	SPDX	Linux Foundation SPDX Project	主にライセンスコンプライアンスを円滑に行うために策定されたフォーマット。セキュリティ対応等にも使える
	SPDX Lite	同上(Open Chain JPWG)	ライセンスコンプライアンスを行うために最低限必要な項目をSPDXから抽出した <b>日本発のヒューマンリーダブルフォーマット</b>
2	SWID tag	NIST(米国国立標準技術研究所)	管理対象機器にインストールされたソフトウェアを追跡するために標準化されたXMLフォーマット
3	CycloneDX	OWASP Foundation	脆弱性対応等のセキュリティ対応を円滑に行うために設計された軽量のSBOM。米国IT企業等での採用例多

Survey of Existing SBOM Formats and Standards  
[https://www.ntia.gov/files/ntia/publications/sbom\\_formats\\_survey-version-2021.pdf](https://www.ntia.gov/files/ntia/publications/sbom_formats_survey-version-2021.pdf)

## SBOMの書き方: SBOMフォーマット

SBOMのグローバル標準は **SPDX/SWID tag/CycloneDX** の3種類  
米バイデン政権の大統領令においても何れかでの提出が求められている

	フォーマット	策定主体	特徴
1	SPDX	Linux Foundation SPDX Project	主にライセンスコンプライアンスを円滑に行うために策定されたフォーマット。セキュリティ対応等にも使える
	SPDX Lite	同上(Open Chain JPWG)	ライセンスコンプライアンスを行うために最低限必要な項目をSPDXから抽出した <b>日本発のヒューマンリーダブルフォーマット</b>
2	SWID tag	NIST(米国国立標準技術研究所)	管理対象機器にインストールされたソフトウェアを追跡するために標準化されたXMLフォーマット
3	CycloneDX	OWASP Foundation	脆弱性対応等のセキュリティ対応を円滑に行うために設計された軽量のSBOM。米国IT企業等での採用例多

Survey of Existing SBOM Formats and Standards  
[https://www.ntia.gov/files/ntia/publications/sbom\\_formats\\_survey-version-2021.pdf](https://www.ntia.gov/files/ntia/publications/sbom_formats_survey-version-2021.pdf)

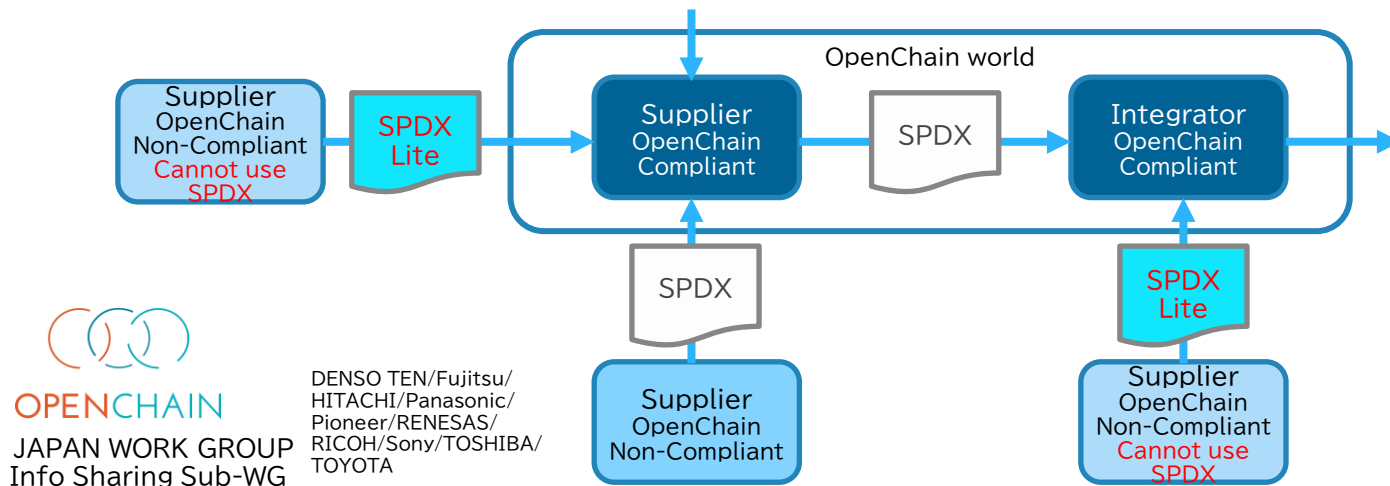
## SPDX-Lite

SPDXのハンドリングが困難な組織でもSBOMを取扱可能にする

入門編のSPDX Liteを定義。Excelで気軽に扱え、ツールとの互換性も確保。

日本からSPDXコミュニティに提案し、

SPDX2.2の1プロファイルとして認められISOの一部に



弊社では、従前よりSBOMフォーマットとして「**SPDX-Lite**」をベースとしてアレンジしたフォーマットで仕入先様よりSBOMを収集しています


→ 当該情報を元にライセンス確認や脆弱性を見ているが、  
増大する情報量とともに情報品質という観点からは限界に来ている

## SBOMは手作業で作る？

先ほどのSPDXなどのフォーマットを使って、手作業で作れなくもないですが現実的にはツールを使うことになる

このツールは「**スキャン(ソフトウェア構成分析)ツール**」と呼ばれます

手作業で作る

ソースから直接・間接的に使われている  
OSSを調査(ライセンス・脆弱性) 

SBOMイメージ

#	コンポーネント	Ver	OSSライセンス	脆弱性	...
1	OSS Lib A	1.2	MIT	高	...
2	OSS Lib B	4.3	GPLv2	低	...
...	...		...	...	...

ツールを使う



#	コンポーネント	Ver	OSSライセンス	脆弱性	...
1	OSS Lib A	1.2	MIT	高	...
2	OSS Lib B	4.3	GPLv2	低	...
...	...		...	...	...

→ OSSが数百ともなると手作業ではもう・・・、脆弱性情報もすぐ古新聞



## ■ スキャンツールは支援、最終判断は人

SBOMを作り出す「**スキャンツール**」は市場にあふれている

有償製品			無償製品(ツール自体OSS)		
Black Duck	FOSSA	FOSSID	Fossology	OSS Review Toolkit	Syft & Gripe
Snyk	Sonatype	Code Insight	trivy	sbom-tool	...
Clarity	Mend.io	SCANOSS			
Cybellum	JFrog Xray	...			

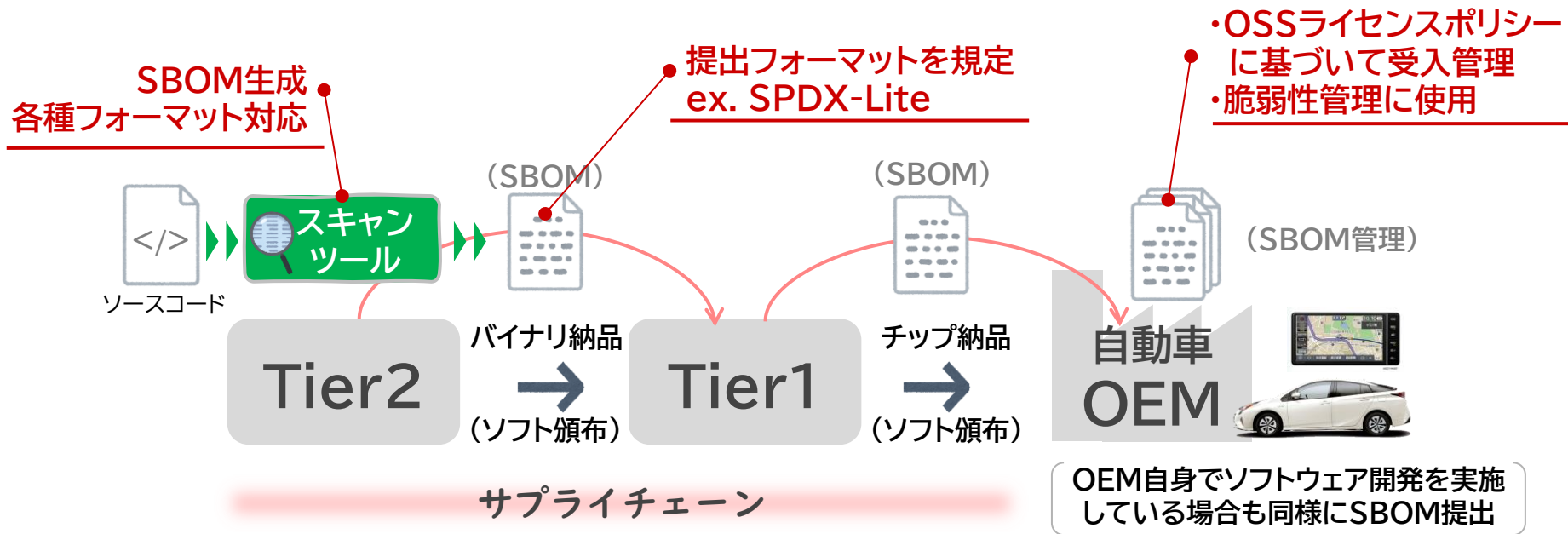
ツールは **万能ではなく、特性を知る** ことが重要です

→ ツールAとツールBの結果が **必ずしも同じとは限りません**

弊社でも**ベンチマークの重要性**を認識、重点取り組み事項の1つ

以上の説明を図にすると

自動車業界にとって **SBOM** は「**リスクマネジメント**」に必須のアイテム  
弊社では、より高度な収集・管理が今後の課題



ご清聴いただきありがとうございました

---



**TOYOTA Open Source**