

? 最近に耳にする「SBOM」って本当に必要なの？

急速にSBOM活用の動きが進んでいます！

自動車業界の動き	Auto-ISAC	「Best Practice Guide – Software Bill of Materials」を公開 (2021年)
	米国運輸省 道路交通安全局	「Cybersecurity Best Practices for the Safety of Modern Vehicles」でSBOMに言及 (2020年)
	自動車メーカー	サプライチェーン全体でのリスク対応においてSBOMフォーマットとしてSPDX-Liteを採用する会社も 参考サイト <a href="https://digitaltrend.hitachi-solutions.co.jp/contents/000209.php">https://digitaltrend.hitachi-solutions.co.jp/contents/000209.php</a>
各国政府の動き	米国	「国家のサイバーセキュリティ改善に関する大統領令」にてSBOMに言及 (2021年)
	EU (欧州連合)	「EUサイバーレジリエンス法」の草案にてSBOM作成の要件が掲載 (2022年)
	日本	経済産業省がSBOM活用促進に向けた実証 (PoC) を開始 (2021年) NISCが「サイバーセキュリティ2022の概要」にてSBOMに言及 (2022年)

詳しくは以下の二次元コードから公式HPを参照してください

※本リーフレット中の会社名、商品名は各社の商標、または登録商標です。 ※本文中および図中では、TMマーク、®マークは表記していません。  
※製品の仕様は、改良のため、予告なく変更する場合があります。 ※本製品を輸出される場合には、外国為替及び外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認の上、必要な手続きをお取りください。なお、ご不明な場合は、当社担当営業にお問い合わせください。 ※本リーフレット中の情報は、作成時点のものです。

株式会社 日立ソリューションズ  
www.hitachi-solutions.co.jp

本リーフレット掲載商品・サービスの詳細情報  
www.hitachi-solutions.co.jp/oms/sp/



当社メンバーが運営する  
「OSS管理ブログ」はこちら！



導入から運用までOSS管理をワンストップで実現

## オープンソース管理ソリューション

### セキュリティ対策の“新常識”

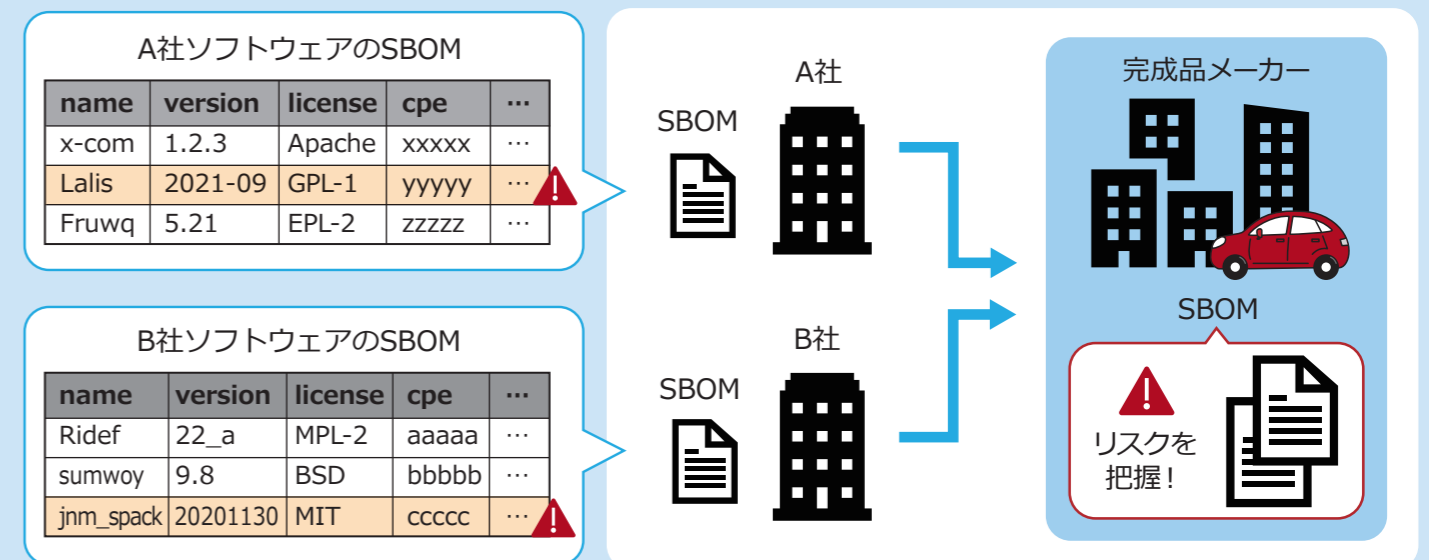
# SBOM

## に対応できていますか？

### SBOM※(ソフトウェア部品表)とは？

※Software Bill of Materials

ソフトウェアにどのような部品(OSSなど)が含まれているかをまとめたデータがSBOMです。SBOMの作成によって、**自社資産のリスクを管理**できるようになります。また、サプライチェーンでのSBOMの共有により、各社の**リスク管理業務を効率化**できます。



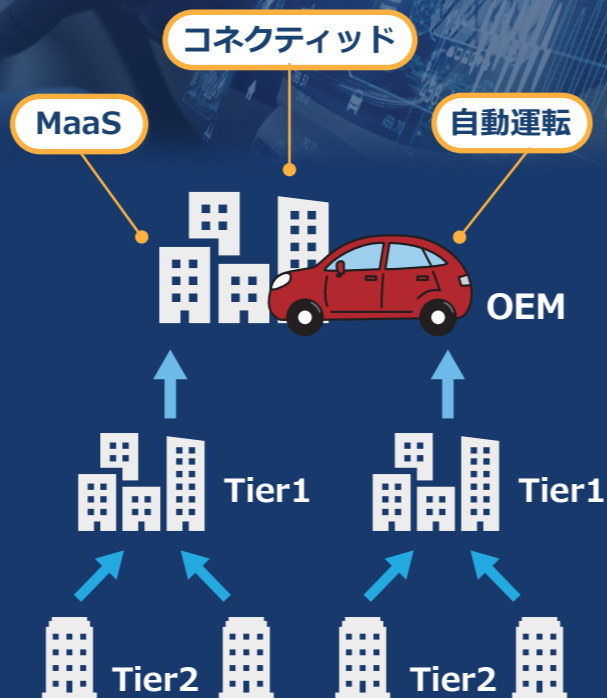
# 自動車業界ではソフトウェアの重要性が拡大。 各社で適切な管理が必要に。

## 1 セキュリティ脆弱性への対応

近年OSS(オープンソースソフトウェア)に由来する脆弱性が多数報告されており、これを狙ったサイバー攻撃が頻発しています。  
車載ソフトウェアでのOSS使用は一般的になっているため、この問題への対応としてSBOMの活用が注目されています。

## 2 サプライチェーン間での情報共有

サプライヤーから納品される製品とそのソフトウェアはブラックボックス化しており、セキュリティやコンプライアンスの問題を内包している可能性があります。  
透明性が高い情報を各社で共有していくために、標準的な仕組みとしてSBOMの使用が推奨されています。



# 多彩なコンサルティングメニューと 先進的なSBOMツールをラインアップ

## SBOM管理ツール

### Black Duck

OSSのソースコードの一部流用を検出する機能(スニペットスキャン)や、Black Duck独自の脆弱性情報(Black Duck Security Advisory)表示などの特長を備えた、高機能な管理ツールです。

### FOSSA

CI/CDツールと連携してパッケージマネージャーの情報からOSSを検出できるなどの特長を備えており、DevSecOpsなどの新しい開発様式にベストマッチの管理ツールです。

### Mend社のソフトウェアコンポジション解析ツール

SaaSで提供されるサービスのため、マシン資産を持たなくてもすぐに使用できます。GUIや出力レポートがグラフィカルで情報を見やすくなっている、などの特長を備えた管理ツールです。

### Insignary Clarity

バイナリファイルを解析することでOSSとそのライセンス・脆弱性などを検出するツールです。ファジーマッチングによって、変更したOSSを含むバイナリファイルも検出が可能です。

## SBOM管理コンサルティング

### SBOM導入支援 / SBOM活用支援

SBOMの代表的なフォーマット(SPDX、CycloneDXなど)の適用や効率的な管理方法・運用ルールの定義、管理ツールの選定などを通して、SBOM管理に必要な仕組みづくりを支援します。

### OSSチェック / SBOM作成支援

お客様の製品のソースコードをお預かりし、それに含まれているOSS、ライセンス、脆弱性などに関してレポートおよびSBOMを作成して、お客様へ提出します。

## OSS管理コンサルティング

### OSS管理プロセス構築支援 / OSPO支援

企業でのOSSの利用ポリシー策定や体制構築などの支援をするサービスです。

### OSSガイドライン策定支援

企業でのOSSのガイドライン策定を支援するサービスです。

### OSS教育

社員のOSSに関する知識レベル向上を目的とし、OSSの基礎から教育を行うものです。

### OSSライセンスに関するコンサルティング

OSSライセンスに関する課題解決を支援するサービスです。

### ISO/IEC 5230(OpenChain)認証

ISO/IEC 5230(OpenChain)の認証取得支援や第三者認証をするサービスです。

### OSSよろず相談

OSSの管理に関する悩みや課題を何でも相談できるサービスです。

## SBOM/OSS管理のことは 日立ソリューションズにご相談ください!

### Point 1 豊富な経験に基づく プロセスコンサル

10年以上にわたりOSSとSBOMの管理に関するコンサルティングを提供。  
お客様の課題に応じた多彩なコンサルティングメニューをご用意しています。

### Point 2 先進的なツールを 複数ラインアップ

SBOM管理ツールの販売、導入支援、活用コンサルティングまでワンストップで提供。複数の製品の中からお客様に最適なものを選択し、ご提案します。

### Point 3 業界への貢献

トヨタ自動車、日立製作所と当社で共同開発した「OSS License Simple Viewer」を公開するなど、業界への貢献と情報発信を積極的に行っています。

### Point 4 唯一の OpenChain<sup>※</sup> 公式パートナー

長年にわたる取り組みが評価され、日本企業として唯一公式パートナーに認定されました。国際標準を熟知したコンサルタントがOSS管理をサポートします。

※OpenChain : OSS 管理の業界標準