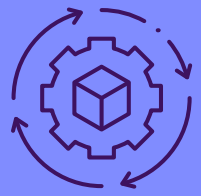
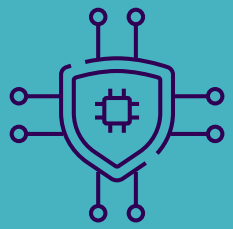
SBOMの導入によるライセンス遵守とソフトウェアセキュリティの強化

The Linux Foundationは、2009年にソフトウェアパッケージデータ交換（SPDX）プロジェクトを立ち上げ、**SBOM標準化に向けた重要なマイルストーンを達成しました。**

アメリカの大統領令14028は、サイバー脅威の高まりに対処するため、**連邦機関がソフトウェア調達にSBOMを使用することを義務付けています。**これにより、**サプライチェーンのセキュリティが強化されます。**





EUの**サイバー レリジエンス法**の重要な要素の一つは、**推奨されるSBOM**の導入であり、製品が設計段階から安全（セキュア バイ デザイン）であることを保証します。

SBOMは、ソフトウェア サプライチェーンを**保護**し、業界や技術領域に関係なく、**国家のサイバーセキュリティ体制を強化します。**

SBOMは包括的で機械可読なインベントリで、アプリケーション、システム、またはソフトウェアスタック内の構成要素となるソフトウェアコンポーネントを詳述しています。

SBOMは通常、**5つの主要な要素**で構成されています。コンポーネント インベントリ、起源情報、依存関係、脆弱性情報、およびメタデータと注釈です。

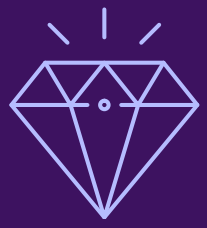
SBOMはライセンス遵守とサイバーセキュリティにおいて重要であり、組織に対してソフトウェア コンポーネントに関する重要な洞察を提供し、**ライセンスの遵守を確保し、サイバー防御を強化します。**

SBOMはライセンス遵守チームに対し、ライセンス違反に伴う**法的、評判的、技術的、および財務的リスクを軽減する**力を与えます。

SBOMは早期警告システムとして機能し、セキュリティリスクの事前軽減を可能にし、インシデントレスポンスやパッチ管理の取り組みを円滑にします。

SBOMの機能は通常、**ソフトウェアコンポジション分析（SCA）ツール**の一部として組み込まれ、オープンソースライセンスの遵守を確保し、コードのセキュリティを向上させます。

効果的な実施のために、組織はSBOMをコンプライアンスおよびセキュリティの実践に統合するのを助ける**明確なポリシーと役割を確立する**必要があります。



組織はSBOMの**定期的かつ適時な更新を行い**、その**実施の効果を監視する**必要があります。