OpenChain Japan Community Day vol.33

HITACHI
Inspire the Next

自動車業界におけるSBOM

- 経産省SBOM実証事業より –

2025/03/03

株式会社日立ソリューションズ
ＩＴプラットフォーム事業部 デジタルアクセラレーション本部 サービスソリューション部
渡邊歩

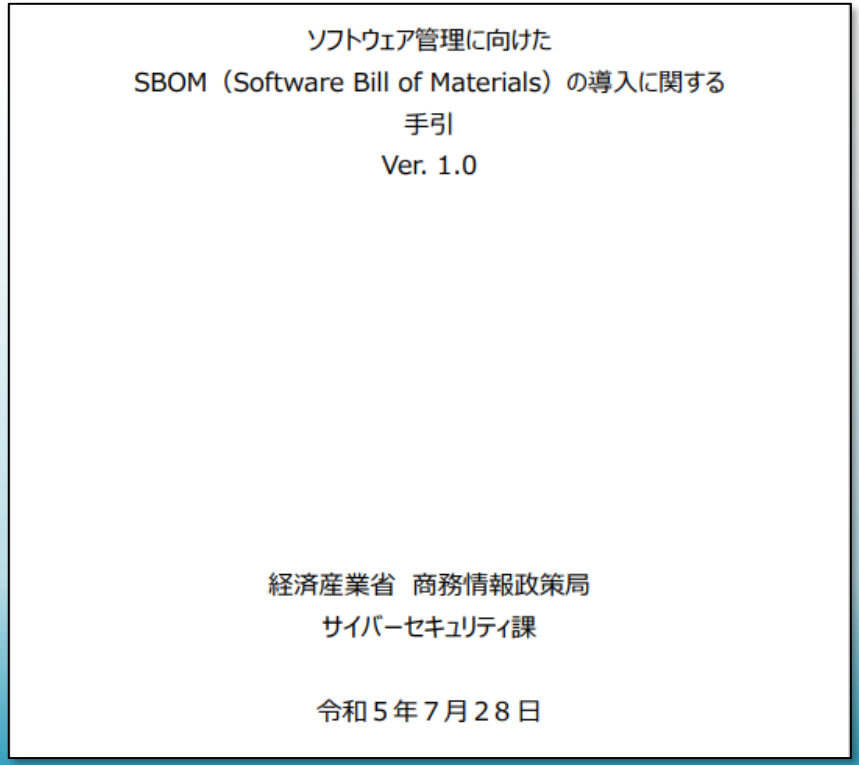
© Hitachi Solutions, Ltd. 2025. All rights reserved.

１．経産省による「SBOM導入に関する手引」

© Hitachi Solutions, Ltd. 2025. All rights reserved.

HITACHI
Inspire the Next

産業界でのSBOM普及促進のため、経済産業省がガイドラインを公開



ソフトウェア管理に向けた
SBOM（Software Bill of Materials）の導入に関する
手引
Ver. 1.0

経済産業省　商務情報政策局
サイバーセキュリティ課

令和５年７月２８日

【手引作成の経緯(経産省における取組み)】

- 2019年に「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」発足
  - ➡ SBOMも含めたソフトウェア管理手法などに関して幅広く議論
- 2021年より、SBOM導入に向けた実証事業を推進
  - ➡ SBOM導入にかかるコストや効果の評価を複数の産業分野で実施

【手引作成の目的】

- SBOMの概要やSBOM導入のメリットなど、SBOMに関する基本的な情報を提供
- SBOM作成に向けた環境構築・体制整備、作成・共有、運用・管理に至る一連のプロセスを提示
  - ➡ ソフトウェア管理に向けたSBOMの作成・共有・運用・管理に関する様々な課題の解決
- 各フェーズにおける主な実施事項やSBOM導入に当たって認識しておくべきポイントを提示
  - ➡ 企業における効率的・効果的なSBOM導入を支援

(https://www.meti.go.jp/press/2023/07/20230728004/20230728004.html)

© Hitachi Solutions, Ltd. 2025. All rights reserved.

1 - 2 経産省のSBOMガイドライン②

政府機関等の対策基準策定のためのガイドライン（令和５年度版）の一部改定（令和６年７月）にて経産省SBOMガイドラインをリファレンス

● **基本対策事項 4.3.1(1)-4「SBOM（Software Bill of Materials：ソフトウェア部品表）」について**

SBOM とは、ソフトウェアコンポーネントに関する情報を含んだ機械処理可能な一覧リストのことで、オープンソースソフトウェアに関する情報だけではなく、プロプライエタリソフトウェア（ソフトウェア配布者がその知的財産を保持しており、改変や複製が制限されているソフトウェア）に関する情報も含めることができる。ソフトウェアに関する選定基準の一つとして、SBOM の情報を機関等が確認できることに関する基準を加えることで、ソフトウェアの透明性の確認を行うことができる。さらに、脆弱性に関する対策の効率化の観点から SBOM を活用することも考えられる。SBOM の項目は多様であり、SBOM の対応範囲に応じてコストと効果が大きく異なるため、分野やシステム利用環境のリスクの違いに応じて妥当な対応範囲を目指すことが効果的である。従って、選定基準においては、SBOM の提供有無の二者択一ではなく、SBOM の対象とするソフトウェアの範囲や脆弱性管理の範囲等について、対象ソフトウェアのリスクを踏まえ、調達先への過度な要求とならない範囲で明示するとよい。例えば、利用時のリスクが低いソフトウェアについては、最小限の SBOM 対応範囲に留めることなどにより、コストを抑えることも考えられる。

SBOM や SBOM 対応範囲の考え方については、経済産業省が公表している以下の手引を参考にするとよい。

参考：経済産業省「ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引」（令和５年７月 28 日）
（https://www.meti.go.jp/press/2023/07/20230728004/20230728004.html）

● **政府機関等のサイバーセキュリティ対策のための統一基準群**

国の行政機関及び独立行政法人等の情報セキュリティ水準を向上させるための統一的な枠組みであり、政府機関等の情報セキュリティのベースラインや、より高い水準の情報セキュリティを確保するための対策事項を規定したもの

● **政府機関等の対策基準策定のためのガイドライン**

統一基準の遵守事項を満たすためにとるべき基本的な対策事項の例示と、対策基準の策定及び実施に際しての考え方等を解説するものであり、政府機関等が、統一基準を遵守するための対策事項として、本ガイドラインを参照しつつ、対策基準を定められるようにするためのもの

7月24日付の一部改訂で追加された部分

(https://www.nisc.go.jp/pdf/policy/general/guider6.pdf)

© Hitachi Solutions, Ltd. 2025. All rights reserved.

1 - 3 経産省のSBOMガイドライン③

HITACHI
Inspire the Next

中小企業を含むあらゆる企業にとってSBOMをより効率的に活用できる方法を盛り込み、改訂版(v2.0)を公開。

【追加された内容】

- **ソフトウェアの脆弱性を管理する一連プロセスにおいてSBOMを効果的に活用するための具体的な手順と考え方をまとめた「脆弱性管理プロセスの具体化」**
- **SBOM導入の効果およびコストを勘案して実際にSBOMを導入することが妥当な範囲を検討するためのフレームワークである「SBOM対応モデル」**
- **委託先との契約などにおいてSBOMに関して規定すべき事項（要求事項、責任、コスト負担、権利など）を示した「SBOM取引モデル」**

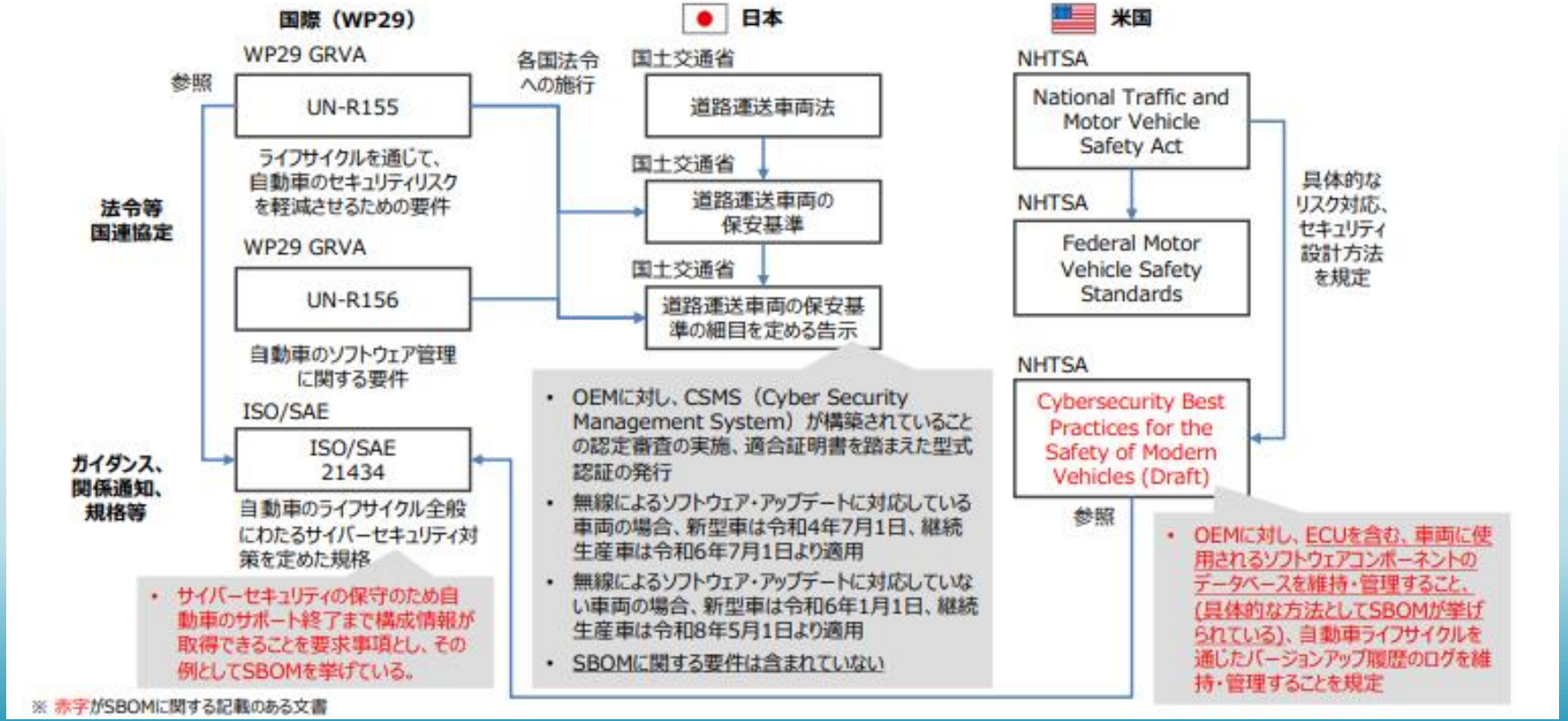
(https://www.meti.go.jp/press/2024/08/20240829001/20240829001-1r.pdf)

© Hitachi Solutions, Ltd. 2025. All rights reserved.

２．自動車業界におけるSBOM

© Hitachi Solutions, Ltd. 2025. All rights reserved.

2-1 自動車分野のSBOMに係る法制度の関係整理



(https://www.meti.go.jp/press/2024/08/20240829001/20240829001-1r.pdf)

© Hitachi Solutions, Ltd. 2025. All rights reserved.

2-2 自動車分野の特徴

分野ごとの前提条件（法制度、取引慣行、開発環境等）の整理

- 産業分野の法制度、取引慣行、開発環境についてSBOMに対する前提状況や要件が異なるため整理する。

前提等	医療機器分野	自動車分野	ソフトウェア分野（情報系）
サプライチェーンの構造	• ソフトウェアの委託開発は一段階層程度が多い • サードパーティ部品（既製品）の構成管理が義務化されており、OSSは対応の困難さから避ける傾向がある。（※ただし、AI/MLを搭載したプログラム医療機器等ではOSSは少なからず利用あり。）	• サプライチェーンは多段階層も多く、中小、海外も含めて裾野が広い。 • サプライチェーンを通じたCSMSが要件化されており、サプライヤに対してもリスク管理のエビデンスが求められる（ISO/SAE21434）。	• 商用、OSS等のサードパーティ部品を使うケースも多い。 • パッケージソフトのサプライチェーンの階層は浅い • 情報システム構築では、多段階層のサプライチェーンも多い。
規制、法制度	• IMDRFガイダンスや米国FDAの市販前ガイダンス案において、既成ソフトウェアコンポーネントに関する機械判読可能なSBOMの生成・提出を推奨。 • IMDRF追補SBOMガイダンス案においてSBOMを推奨化しており、日本もそれに整合する方向性。 • 構成管理は医療機器の基本要件基準第12条第2項の適用。第3項にサイバーセキュリティ要件新設予定。 • 業の許認可がある。	• 日欧など型式認証で要求される国連協定規則UN-R155から参照されるISO/SAE21434では、構成管理が要求され、例としてソフトウェア部品表の作成が挙げられる。 • 米国NHTSAガイダンス(2021年)により、OEMやサプライヤーに対して、ECUや各車両のソフトウェアに関するSBOMの作成・維持が推奨される	• 米国大統領令に基づき、連邦政府のソフトウェア調達においてSBOMを開示等することが義務化される見通し(2022年度内)。
開発対象・開発環境等	• C/C++が多く、アセンブラ、Java、Pythonも利用実績あり。 • AI/MLを搭載したプログラム医療機器ではOSS利用もあり。 • Nessus（脆弱性チェックツール）がFDA対応でよく用いられる。	• 制御系でC/C++/アセンブラが多い。 • 情報系でOSSの利用増加が見込まれる • ECUの場合、納品はバイナリ/ソースコードの両ケースがある。 • 構成管理ツールとして、Git, Subversionなど利用するケースがある。	• Java，C/C++，Python、JavaScriptなどを含め多様な開発言語 • SaaS等のクラウドやオンプレミスなど • ビルド・構成管理ツールはJenkins,GitHubなど、開発環境は，VisualStudio，Eclipseなどが多い
取引慣行・契約	• 開発委託、保守委託が多い。 • 市販後は修理業が対応する場合もある。	• 請負契約、準委任契約など各種存在。 • OSS使用については報告を要件化する場合あり • 脆弱性の監視と連絡を要件化する場合あり	• ユーザ向けライセンス契約あり • 将来の部品情報、SBOMの提供は要件化の有無は両ケースあり
実証の論点	• サードパーティの再帰的な利用部品などの精度の高いSBOM作成 • 脆弱性管理プロセスへの対応における課題	• 商用部品、OSS等のSBOMの現実的な生成範囲 • サプライチェーンを通じたSBOM共有と迅速な脆弱性対応	• 商用部品、OSSのサプライヤーに依存しないSBOM作成 • 開発環境、開発言語のSBOMツールへの影響

(https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/009_03_00.pdf)

© Hitachi Solutions, Ltd. 2025. All rights reserved.

2 - 3 実証で抽出された主な課題と解決策

HITACHI
Inspire the Next

区分	実証から抽出した課題	解決ノウハウ	今後の課題(国、民間)	医療機器	自動車	ソフトウェア
技術	検出した脆弱性の対応要否、優先度の判断が困難	医療機器分野の脆弱性対応フローなどを参考にアドバイザリー、脅威情報を活用し、対応の要否、優先度を判断	脆弱性管理の高度化、脅威情報の普及促進	●		
	SBOMツールの使い分け・変更による負担増大	機能ニーズを洗い出し、ツール比較情報をもとに選択	-	●	●	●
	CI/CDなど継続的なアップデートへの対応負担	ツールによる自動化可能な範囲で管理	CI/CDに対応した自動管理			●
	SBOM初期導入、ツールなどのコスト負担が大きい	ツールの効率的な導入方法、OSSツールの選択活用	OSSベースのツール整備	●	●	●
管理	SBOMに要求される精査のレベルが不明確	SBOM対応モデルの選択肢やSBOMツールの機能に応じて精査の要否を判断する	-	●	●	
	SBOM生成の対象範囲が不明確	OS, ミドルウェアを含めて対象全体の上位構成を事前に明確化	-	●	●	●
	ツールの環境構築、SBOM共有のコストが大きい	SaaS型SBOMツールで初期導入と共有の工数を低減	サプライチェーンを通じた脆弱性管理	●	●	●
	ユーザー組織によるSBOMの活用・管理が困難	SBOMツール導入、ベンダー支援の活用	-	●	●	●
	部品の脆弱性残存期間に応じたリスク評価	SBOMの履歴管理により脆弱性残存期間を特定	脆弱性の履歴評価			●
	開発部署、PSIRTなどの部署ごとの脆弱性管理が非効率	社内でSBOMを一元管理することで、脆弱性管理を効率化	SBOMによる脆弱性の社内一元管理		●	●
	サプライヤーごとの部品粒度のバラつき	取得したすべての粒度をツールで自動管理	脆弱性マッチングの高度化		●	
	サプライヤーのサポート切れなどのリスク対応	部品のEoLなどに基づくサポート計画・管理を実施	-	●		
取引	サードパーティーからのSBOM取得が困難、バイナリ納品物の脆弱性の監視・修正が負担	ソースコード取得とSBOMツールの適用、(バイナリ納品の場合)SBOM提供と脆弱性修正を契約で要件化	-	●	●	●
	サプライヤー部品の精査コストが大きい	SBOMの提供と信頼性に関する責任を契約で規定	-	●	●	

※CI/CD ・・・ 継続的インテグレーション/継続的デリバリー　※PSIRT ・・・ Product Security Incident Response Team

© Hitachi Solutions, Ltd. 2025. All rights reserved.

HITACHI
Inspire the Next

SBOMの効果的な対応案（自動車分野：東海理化等）

- 自動車分野では、法制度上、構成管理が求められている。
- 法制度や取引慣行、実証結果を踏まえると、下記表のとおり、より効果的に活用していくための課題及び対応等が考えられるところ、これを案として自動車業界と調整を図っていく。

SBOM対応項目	実証結果	より効果的に活用していくための課題や考えられる対応など
作成主体	開発委託先にもSBOMを要件化可能。サードパーティについてはSBOM提供は無く、コードレビューにより部品の特定を実施。	法制度上、構成管理が求められるため、開発委託先にもSBOMを要件化する。OSSなどサードパーティからSBOM取得ができ無い場合、委託先の開発者が部品を特定し、委託元に対して利用するOSS の申告と合意を得る。 →今後、策定する取引モデルの活用の検討。
作成範囲（カバレッジ）	直接利用部品の作成は可能。間接利用部品はパッケージマネージャの構成情報などを用いて効率的に実施できる部分は対応。	直接利用部品の作成必須。間接利用部品は、ツールやレビューにより可能な範囲で作成する。 →業界におけるコンセンサス形成の検討、SBOM取引モデルに基づいた受発注者間の契約の検討など
精査（信頼性確保）	ツールの誤検出があるため、精査は必要。効率的に精査可能な直接利用部品について実施可能。	ツールだけでは誤検出があるため、効率的に精査可能な部品については実施。 →取引モデル等の活用により、受発注者間で契約などを締結することの検討、ツールの構成解析機能（依存関係解析、スニペット解析、ファイル照合等）に応じて、誤検知、検出漏れ有無を判断し、コードレビューなどにより効率的な精査の方法の検討。
活用範囲	脆弱性・ライセンスの特定まで可能。深刻度評価、悪用可能性評価はツール無しではコストが大きい。	脆弱性・ライセンスの特定までとし、深刻度評価、悪用可能性評価はリスクの大きい場合に限定 →ISAC,ベンダーからのVEX文書の活用方法の組織導入の検討
フォーマット	SPDX(ツール出力)	－

24

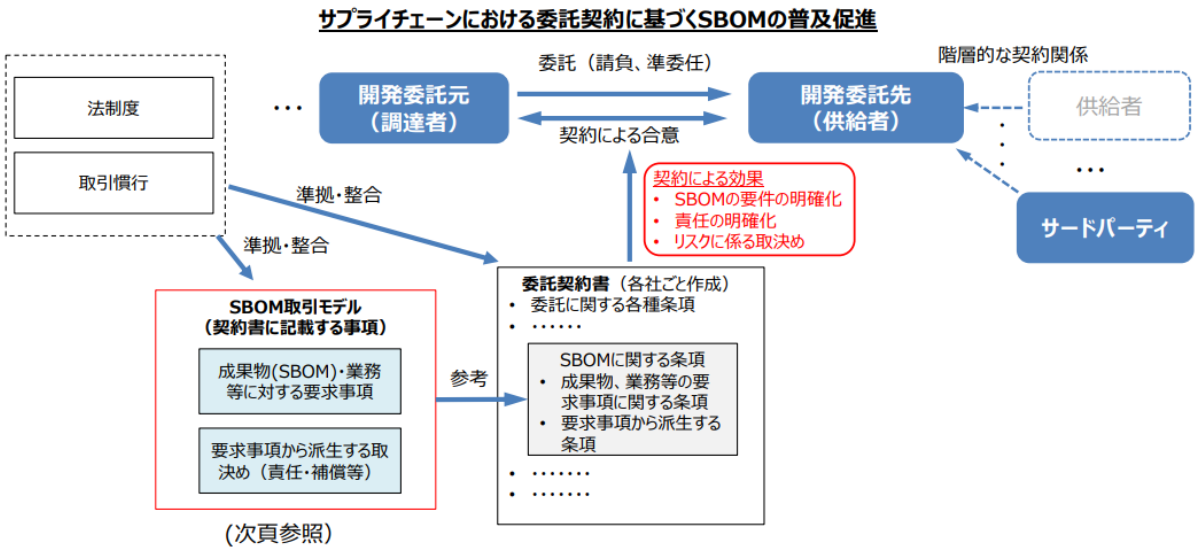
(https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/009_03_00.pdf)

© Hitachi Solutions, Ltd. 2025. All rights reserved.

2 - 5 SBOM取引モデル①

SBOM取引モデルの意義と位置付け（全体像）

- SBOMのメリットは、サプライチェーンを通じて標準化された部品情報の共有と自動処理による効率化が挙げられる。特にSBOMを受け取る委託元の便益は大きいが、委託先はそのために追加負担を強いられることもあり、受発注者間で得られる便益が異なる。
- そのようなことから、サプライチェーンを通じたSBOMの普及のためには、受発注者間で得られる便益に応じた対価負担の取決めが必要であり、委託契約において、SBOMの対応範囲とそれに対する対価負担、責任の明確化が必要。
- SBOM取引モデルは、そのようなSBOMに対する要求事項と派生する対価負担、責任関係について取り決める事項を示すものである。SBOM取引モデルは各社ごとの契約書作成において参考となり、SBOMの効果的な利活用に資するものである。



28

© Hitachi Solutions, Ltd. 2025. All rights reserved.

2-6 SBOM取引モデル②

ver2.0追加内容

SBOM取引モデルの概要

SBOM取引モデルの主な構成要素（契約で規定することが期待される事項）

- 契約で規定すべき事項として、SBOMに関する要求事項、責任、コスト負担、権利などの区分で整理される。業界の取引慣行、タスクフォース意見を網羅するように整理。脆弱性管理、ソフトウェア品質保証に重要な要件を言語化。主に要件定義後の請負契約が対象と想定。

区分		規定すべき事項	レベル
SBOM要求事項	フォーマット・標準	**（SBOMフォーマット）※1** 採用するSBOM標準フォーマットについて規定する。（SPDX, CycloneDX, SWID等の標準とバージョンを規定）	基礎
		（ID標準）※1 採用する部品ID標準を規定する。（CPE, PURL, SWD, 独自形式等）	基礎
		（SBOM最小要素）※1 採用するSBOMフォーマットの要素項目のうち最小要素を規定する。NTIAのSBOM最小要素を参考にする。	基礎
	品質・信頼性 （SBOM対応モデルに該当）	**（対象サプライヤ契約形態）** SBOM作成範囲として、委託開発契約、サードパーティ利用規約（商用既製品、OSS）の契約形態による範囲を規定する。	基礎
		（再帰的利用部品）※1 SBOM作成範囲として、直接利用部品か再帰的な間接利用部品までとするか規定する。	発展
		（構成解析手法の適用範囲）※1 間接利用部品について、部品を特定する際に利用する構成解析手法の適用範囲を規定する。（依存関係解析、ファイル照合、スニペット解析等）	発展
		（部品精査の要否）※1 ツールによる部品特定の結果に対して、手動による誤検知・検出漏れの精査の要否を規定する。	発展
		（部品の対象フェーズ）※1 部品情報の範囲としてビルド時、ランタイム、クラウドサービス等の範囲を規定する。	発展
		（サードパーティ部品の事前合意） サードパーティ部品（商用部品、OSS）を利用する場合、事前の申告と合意の要否について規定する。	基礎
	保守・運用	**（共有方法）※1** SBOMファイルによる授受またはSaaS等によるリアルタイム共有について規定する。	基礎
		（VEX対応）※1 SBOMに関連する脆弱性情報について悪用可能性に基づくVEX情報の提供を行うか規定する。	発展
		（SBOM更新）※1 ソフトウェアのアップデート、SBOM不具合修正等に応じて、SBOMを更新する期限や頻度を規定する。	基礎
		（脆弱性監視・通知） ソフトウェアの運用フェーズにおいて、脆弱性を監視し、脆弱性が発見された場合に、調達者に通知の期限を規定する。	発展
		（脆弱性対応・優先付け）※1 脆弱性が発見された際に、脆弱性対応の要否、優先付け（トリアージ）について調達者に情報提供を行うか規定する。	発展
		（EOL・EOS） サードパーティ部品および委託開発部品のEOL、EOSやその期限変更に対する通知について規定する。	発展
責任と保証		**（エビデンス提出）** SBOM要求事項について適合していることを証明するエビデンス、第三者証明の提出の要否について規定する。	発展
		（契約不適合責任） SBOM要求事項に対する不適合が見つかった場合には、SBOM修正等の瑕疵対応の要否について規定する。	基礎
		（損害賠償）※2 SBOM要求事項の不適合が原因で事故が発生した場合、損害賠償額上限等について規定する。ライセンス違反の損害賠償を含む。	基礎
		（免責） SBOM要求事項への適合性エビデンスを提出している場合について、技術的制約（ツールの誤検知など）に帰する理由で、損害が発生した場合について損害賠償の制限、免責について規定する。	発展
コスト負担		**（見積）※2** SBOM要求事項、責任・保証に基づき見積の作成し、その合意金額に基づき対価支払について規定する。	基礎
権利・機密保持		**（知的財産権の帰属）** 作成したSBOMの知的財産権、使用権の帰属、第三者への提供可否について規定する。	発展
		（機密保持） SBOMの機密保持・管理およびSBOMを用いたリバースエンジニアリングの禁止について規定する。	発展

凡例：基礎 分野共通で最低限期待される事項
発展 特定分野、要求レベルの高い分野で期待される事項

※1 発注仕様書に記載することも想定される。
※2 ソフトウェア開発一般の請負契約と共通化することが想定される。

9

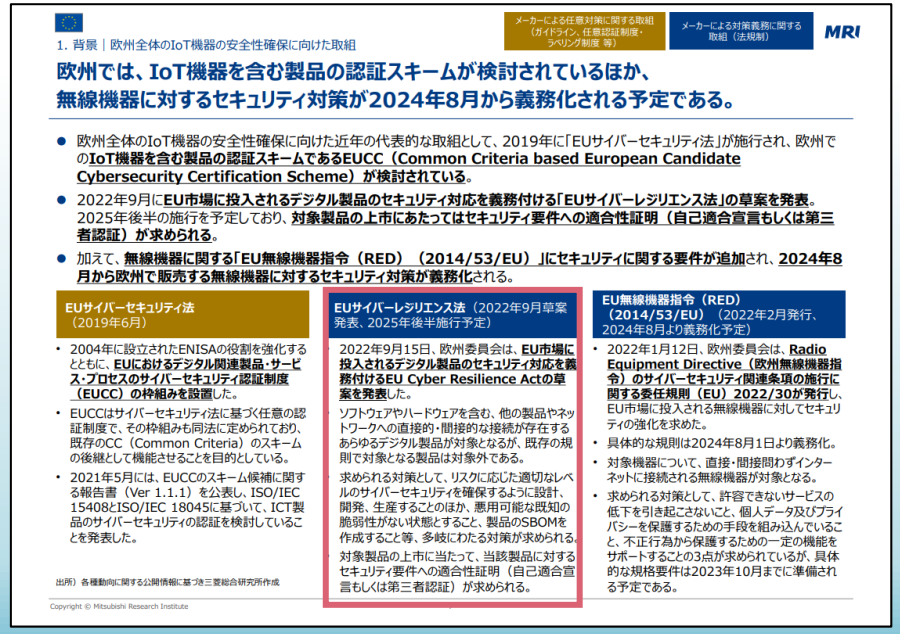
(https://www.meti.go.jp/press/2024/08/20240829001/20240829001-2.pdf)

© Hitachi Solutions, Ltd. 2025. All rights reserved.

3. 今後の動向

© Hitachi Solutions, Ltd. 2025. All rights reserved.

EUサイバーレジリエンス法によりSBOMによるセキュリティ対策が必須化



1. 背景｜欧州全体のIoT機器の安全性確保に向けた取組

メーカーによる任意対策に関する取組（ガイドライン、任意認証制度・ラベリング制度 等）

メーカーによる対策義務に関する取組（法規制）

MRI

欧州では、IoT機器を含む製品の認証スキームが検討されているほか、無線機器に対するセキュリティ対策が2024年8月から義務化される予定である。

- 欧州全体のIoT機器の安全性確保に向けた近年の代表的な取組として、2019年に「EUサイバーセキュリティ法」が施行され、欧州の**IoT機器を含む製品の認証スキームであるEUCC（Common Criteria based European Candidate Cybersecurity Certification Scheme）が検討されている**。
- 2022年9月に**EU市場に投入されるデジタル製品のセキュリティ対応を義務付ける「EUサイバーレジリエンス法」の草案を発表**。2025年後半の施行を予定しており、**対象製品の上市にあたってはセキュリティ要件への適合性証明（自己適合宣言もしくは第三者認証）が求められる**。
- 加えて、**無線機器に関する「EU無線機器指令（RED）（2014/53/EU）」にセキュリティに関する要件が追加**され、**2024年8月から欧州で販売する無線機器に対するセキュリティ対策が義務化**される。

EUサイバーセキュリティ法（2019年6月）

- 2004年に設立されたENISAの役割を強化するとともに、**EUにおけるデジタル関連製品・サービス・プロセスのサイバーセキュリティ認証制度（EUCC）の枠組みを設置**した。
- EUCCはサイバーセキュリティ法に基づく任意の認証制度で、その枠組みも同法に定められており、既存のCC（Common Criteria）のスキームの後継として機能させることを目的としている。
- 2021年5月には、EUCCのスキーム候補に関する報告書（Ver 1.1.1）を公表し、ISO/IEC 15408とISO/IEC 18045に基づいて、ICT製品のサイバーセキュリティの認証を検討していることを発表した。

EUサイバーレジリエンス法（2022年9月草案発表、2025年後半施行予定）

2022年9月15日、欧州委員会は、**EU市場に投入されるデジタル製品のセキュリティ対応を義務付けるEU Cyber Resilience Actの草案を発表**した。

ソフトウェアやハードウェアを含む、他の製品やネットワークへの直接的・間接的な接続が存在するあらゆるデジタル製品が対象となるが、既存の規則で対象となる製品は対象外である。

求められる対策として、リスクに応じた適切なレベルのサイバーセキュリティを確保するように設計、開発、生産することのほか、悪用可能な既知の脆弱性がない状態とすること、製品のSBOMを作成すること等、多岐にわたる対策が求められる。

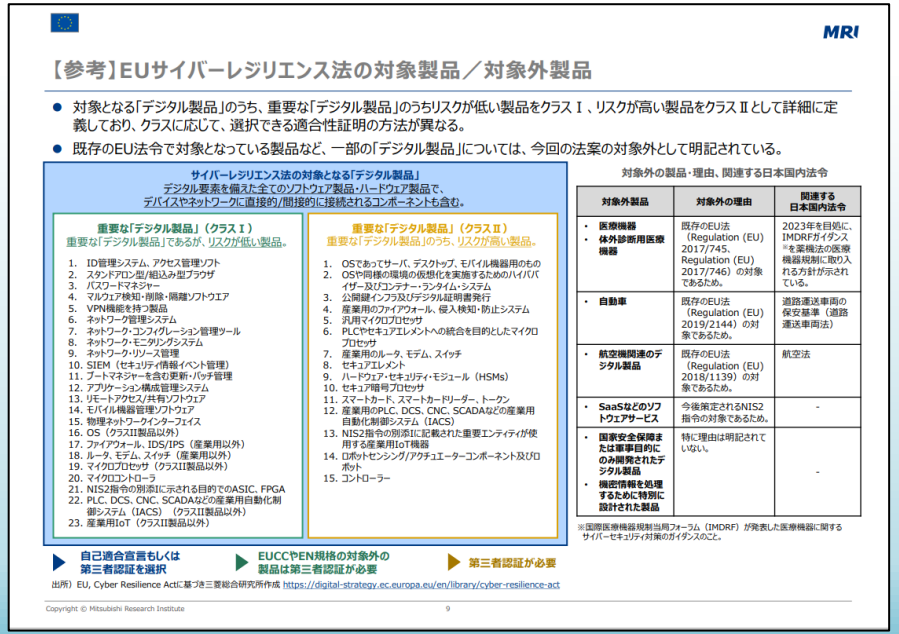
対象製品の上市に当たって、当該製品に対するセキュリティ要件への適合性証明（自己適合宣言もしくは第三者認証）が求められる。

EU無線機器指令（RED）（2014/53/EU）（2022年2月発行、2024年8月より義務化予定）

- 2022年1月12日、欧州委員会は、**Radio Equipment Directive（欧州無線機器指令）のサイバーセキュリティ関連条項の施行に関する委任規則（EU）2022/30が発行**し、EU市場に投入される無線機器に対してセキュリティの強化を求めた。
- 具体的な規則は2024年8月1日より義務化。
- 対象機器について、直接・間接問わずインターネットに接続される無線機器が対象となる。
- 求められる対策として、許容できないサービスの低下を引き起こさないこと、個人データ及びプライバシーを保護するための手段を組み込んでいること、不正行為から保護するための一定の機能をサポートすることの3点が求められているが、具体的な規格要件は2023年10月までに準備される予定である。

出所）各種動向に関する公開情報に基づき三菱総合研究所作成

Copyright © Mitsubishi Research Institute



MRI

【参考】EUサイバーレジリエンス法の対象製品／対象外製品

- 対象となる「デジタル製品」のうち、重要な「デジタル製品」のうちリスクが低い製品をクラスⅠ、リスクが高い製品をクラスⅡとして詳細に定義しており、クラスに応じて、選択できる適合性証明の方法が異なる。
- 既存のEU法令で対象となっている製品など、一部の「デジタル製品」については、今回の法案の対象外として明記されている。

サイバーレジリエンス法の対象となる「デジタル製品」
デジタル要素を備えた全てのソフトウェア製品・ハードウェア製品で、デバイスやネットワークに直接的/間接的に接続されるコンポーネントも含む。

重要な「デジタル製品」（クラスⅠ）
重要な「デジタル製品」であるが、リスクが低い製品。

1. ID管理システム、アクセス管理ソフト
2. スタンドアロン型/組込み型ブラウザ
3. パスワードマネジャー
4. マルウェア検知・削除・隔離ソフトウエア
5. VPN機能を持つ製品
6. ネットワーク管理システム
7. ネットワーク・コンフィグレーション管理ツール
8. ネットワーク・モニタリングシステム
9. ネットワーク・リソース管理
10. SIEM（セキュリティ情報イベント管理）
11. ブートマネジャーを含む更新・パッチ管理
12. アプリケーション構成管理システム
13. リモートアクセス/共有ソフトウェア
14. モバイル機器管理ソフトウェア
15. 物理ネットワークインターフェイス
16. OS（クラスII製品以外）
17. ファイアウォール、IDS/IPS（産業用以外）
18. ルータ、モデム、スイッチ（産業用以外）
19. マイクロプロセッサ（クラスII製品以外）
20. マイクロコントローラ
21. NIS2指令の別添Iに示される目的でのASIC、FPGA
22. PLC、DCS、CNC、SCADAなどの産業用自動化制御システム（IACS）（クラスII製品以外）
23. 産業用IoT（クラスII製品以外）

重要な「デジタル製品」（クラスⅡ）
重要な「デジタル製品」のうち、リスクが高い製品。

1. OSであってサーバ、デスクトップ、モバイル機器用のもの
2. OSや同様の環境の仮想化を実施するためのハイパバイザー及びコンテナー・ランタイム・システム
3. 公開鍵インフラ及び/デジタル証明書発行
4. 産業用のファイアウォール、侵入検知・防止システム
5. 汎用マイクロプロセッサ
6. PLCやセキュアエレメントへの統合を目的としたマイクロプロセッサ
7. 産業用のルータ、モデム、スイッチ
8. セキュアエレメント
9. ハードウェア・セキュリティ・モジュール（HSMs）
10. セキュア暗号プロセッサ
11. スマートカード、スマートカードリーダー、トークン
12. 産業用のPLC、DCS、CNC、SCADAなどの産業用自動化制御システム（IACS）
13. NIS2指令の別添Iに記載された重要エンティティが使用する産業用IoT機器
14. ロボットセンシング/アクチュエーターコンポーネント及びロボット
15. コントローラー

▶ 自己適合宣言もしくは第三者認証を選択　▶ EUCCやEN規格の対象外の製品は第三者認証が必要　▶ 第三者認証が必要

出所）EU, Cyber Resilience Actに基づき三菱総合研究所作成 https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

対象外の製品・理由、関連する日本国内法令

対象外製品	対象外の理由	関連する日本国内法令
• 医療機器 • 体外診断用医療機器	既存のEU法（Regulation (EU) 2017/745、Regulation (EU) 2017/746）の対象であるため。	2023年を目処に、IMDRFガイダンス※を薬機法の医療機器規制に取り入れる方針が示されている。
• 自動車	既存のEU法（Regulation (EU) 2019/2144）の対象であるため。	道路運送車両の保安基準（道路運送車両法）
• 航空機関連のデジタル製品	既存のEU法（Regulation (EU) 2018/1139）の対象であるため。	航空法
• SaaSなどのソフトウェアサービス	今後策定されるNIS2指令の対象であるため。	-
• 国家安全保障または軍事目的にのみ開発されたデジタル製品 • 機密情報を処理するために特別に設計された製品	特に理由は明記されていない。	-

※国際医療機器規制当局フォーラム（IMDRF）が発表した医療機器に関するサイバーセキュリティ対策のガイダンスのこと。

Copyright © Mitsubishi Research Institute

EU市場に投入されるデジタル製品について、製品のSBOMを作成することなどを義務付ける
違反時には膨大な過料(1.500万ユーロ(約23.5億円)またはグローバルの売り上げの2.5%のいずれか高い方)が課せられる

出典：三菱総合研究所「IoT製品に対するセキュリティ適合性評価制度の構築について」

© Hitachi Solutions, Ltd. 2025. All rights reserved.

3 - 2 業界団体によるガイダンス

HITACHI
Inspire the Next

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Feb 11

AUTO-ISAC ISSUES "SOFTWARE BILL OF MATERIALS" INFORMATIONAL REPORT

Advancing Cybersecurity for the Connected Vehicle Industry

Washington, DC – February 11, 2025 – The Automotive Information Sharing and Analysis Center (Auto-ISAC) today announced the public release of its groundbreaking Auto-ISAC Software Bill of Materials (SBOM) Informational Report with effective practices to enhance the software security of automotive vehicles, products, and technology. The report can be obtained through the Auto-ISAC's public website at www.automotiveisac.com.

A Software Bill of Materials (SBOM) is a structured, hierarchical list of software libraries and other components that make up a software product. The Auto-ISAC SBOM Informational Report details key insights and guidance specifically tailored for the automotive industry to enhance transparency and knowledge of software products, while helping different parts of an organization collaborate more effectively through sharing the same understanding of software products.

(https://automotiveisac.com/press-news/auto-isac-issues-software-bill-of-materials-informational-report-nbsp)

© Hitachi Solutions, Ltd. 2025. All rights reserved.

HITACHI
Inspire the Next

米商務省、中国とロシアが関係するコネクテッドカーの輸入・販売を禁止する最終規則を発表

News & Updates › Press Releases › Commerce Finalizes Rule to Secure Connected Vehicle Supply Chains from Forei…

Bureau of Industry & Security

Office of Congressional and Public Affairs

FOR IMMEDIATE RELEASE | Tuesday, January 14, 2025 | Media Contact: OCPA@bis.doc.gov

Commerce Finalizes Rule to Secure Connected Vehicle Supply Chains from Foreign Adversary Threats

Download as PDF

Washington, D.C. – Today, the U.S. Department of Commerce's Bureau of Industry and Security (BIS) announced a final rule prohibiting certain transactions involving the sale or import of connected vehicles integrating specific pieces of hardware and software, or those components sold separately, with a sufficient nexus to the People's Republic of China (PRC) or Russia.

BIS and its Office of Information and Communications Technology and Services (OICTS) have found that certain technologies originating from the PRC or Russia present an undue and unacceptable risk to U.S. national security. Today's action represents the culmination of a months-long regulatory process to design, seek public input on, and ultimately finalize a measure to protect drivers and passengers on American roads.

(https://www.bis.gov/press-release/commerce-finalizes-rule-secure-connected-vehicle-supply-chains-foreign-adversary)

© Hitachi Solutions, Ltd. 2025. All rights reserved.

本資料に記載されている会社名、製品名は、それぞれの各社の商号、商標もしくは登録商標です。

HITACHI
Inspire the Next

END

自動車業界におけるSBOM
- 経産省SBOM実証事業より –

2025/03/03

株式会社日立ソリューションズ
ＩＴプラットフォーム事業部 デジタルアクセラレーション本部 サービスソリューション部
渡邊歩

© Hitachi Solutions, Ltd. 2025. All rights reserved.