HITACHI
Inspire the Next

サプライチェーンを可視化するSBOMとは

2023/06/09

日立チャネルソリューションズ株式会社
コア技術開発センタ　ソリューション技術開発本部　ソリューション技術開発部／技師

一般社団法人　重要生活機器連携セキュリティ協議会（CCDS）
研究開発センター／シニアリサーチャー

石川 智祥

HITACHI
Inspire the Next

Contents

1. サプライチェーンセキュリティ
2. SBOM（Software Bill of Materials）とは
3. SBOMを取り巻く状況
4. SBOMの導入

日立チャネルソリューションズ株式会社

HITACHI
Inspire the Next

会社名	日立チャネルソリューションズ株式会社 Hitachi Channel Solutions, Corp.
本社所在地	東京本社：東京都品川区 旭本社：愛知県尾張旭市
資本金	85億円
設立	2004年10月
従業員数	単独：907名　連結：2，042名　（2023年3月末現在）
事業内容	情報機器、メカトロ機器の企画、開発、設計、製造、販売およびサービス・ソリューションの提供
URL	https://www.hitachi-ch.co.jp/

製品・サービス

金融機関

ATM「AKe-S」

営業店システム

公共・交通

座席予約端末装置

ヘルスケア

自動受付精算機

自己紹介

HITACHI
Inspire the Next

石川 智祥

日立チャネルソリューションズ株式会社
コア技術開発センタ
ソリューション技術開発本部
ソリューション技術開発部／技師

一般社団法人
重要生活機器連携セキュリティ協議会(CCDS)
研究開発センター／シニアリサーチャー

・情報処理安全確保支援士(登録番号 第006397号)

主な略歴

2007年　CEN/XFSワークショップ活動開始
2007年　セキュリティ系業務開始
2015年　CCDSプロジェクト参加
2021年　CCDS出向(～2022年)

CEN:
欧州標準化委員会

CEN/XFS:
ATM(現金預け払い機)におけるミドルウェアのグローバル標準インタフェース

一般社団法人　重要生活機器連携セキュリティ協議会（CCDS）

HITACHI
Inspire the Next

設立:　2014年10月6日
会長:　徳田英幸（情報通信研究機構　理事長、慶応大学 名誉教授）
代表理事: 荻野 司（情報セキュリティ大学院大学　客員教授）
理事:　江崎 浩（東京大学大学院 教授）
　　後藤 厚宏（情報セキュリティ大学院大学 学長）
　　松本 勉（横浜国立大学先端科学高等研究院 教授）
会員数: 203(正会員以上:49、一般会員:124、学術系:17、協賛:17)(2023年5月)
主な事業:

1. 生活機器の各分野におけるセキュリティに関する国内外の動向調査、内外諸団体との交流・協力
2. 生活機器の安全と安心を両立するセキュリティ技術の開発
3. セキュリティ設計プロセスの開発や検証方法のガイドラインの開発、策定および国際標準化の推進
4. 生活機器の検証環境の整備・運用管理及び検証事業、セキュリティに関する人材育成や広報・普及啓発活動等

「IoT社会に対応したサイバー・フィジカル・セキュリティ」

HITACHI
Inspire the Next

戦略的イノベーション創造プログラム(SIP)第2期(2018年度～2022年度)のプログラムの1つ

- 研究推進法人として、国立研究開発法人 新エネルギー・産業技術総合開発機構(NEDO)が担当
- NEDOが当プロジェクトの一環として公募した2案件をCCDSが受託

NEDOの「IoT社会に対応したサイバー・フィジカル・セキュリティ」ポータルサイト

NEDO.「戦略的イノベーション創造プログラム(SIP)第2期／IoT社会に対応したサイバー・フィジカル・セキュリティ」.
https://www.nedo.go.jp/activities/ZZJP2_100123.html, (参照 2023-05-31)

本プレゼンテーション資料の内容について

HITACHI
Inspire the Next

NEDOからの委託を受けて、CCDSが以下の成果報告書をまとめた際の調査の内容を含みます。

◇「戦略的イノベーション創造プログラム（SIP）第2期／IoT社会に対応したサイバー・フィジカル・セキュリティ／IoT社会に対応したサイバー・フィジカル・セキュリティに係るOSSの技術検証のあり方等に関する調査」、NEDO、2021年度～2022年度、報告書管理番号：20220000000436
https://www.nedo.go.jp/content/100953488.pdf

◇「戦略的イノベーション創造プログラム（SIP）第2期／IoT社会に対応したサイバー・フィジカル・セキュリティ／IoT社会に対応したサイバー・フィジカル・セキュリティに係るOSSの管理手法及びCSIRT・PSIRT連携等に関する調査」、NEDO、2022年度～2022年度、報告書管理番号：20220000001048
https://www.nedo.go.jp/content/100956036.pdf

※商標について
本プレゼンテーション資料に記載の会社/組織名、製品名などは、各社/各組織の商標または登録商標です。

1. サプライチェーンセキュリティ

HITACHI
Inspire the Next

サプライチェーンを狙ったサイバー攻撃が増えている

サプライチェーンを狙ったサイバー攻撃を伝える記事

日本経済新聞	供給網のサイバー攻撃、対策済みは3割　民間調べ https://www.nikkei.com/article/DGXZQOUC25DAV0V20C22A8000000/ （2022年8月26日）
NHK	サイバー攻撃受けた病院 給食業者経由でウイルス侵入か 大阪 https://www3.nhk.or.jp/kansai-news/20221107/2000068042.html （2022年11月7日）
Bloomberg	日本で急増するサイバー攻撃、世界サプライチェーンリスク浮き彫りに https://www.bloomberg.co.jp/news/articles/2023-04-19/RTAEGJT0AFB401 （2023年4月19日）

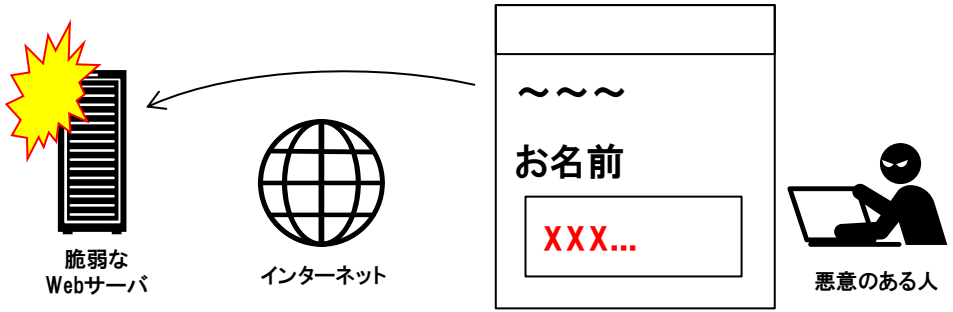
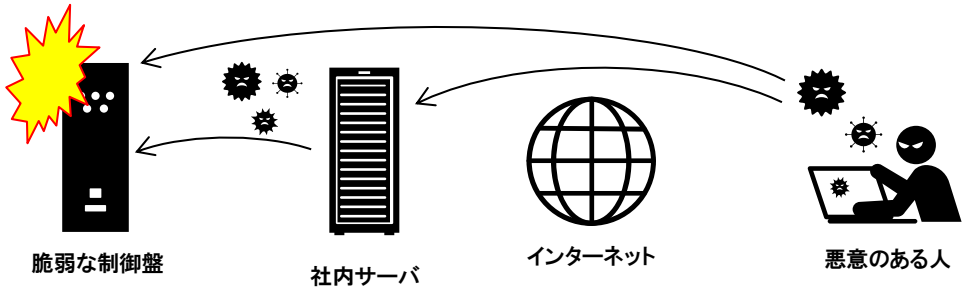
IPA「情報セキュリティ10大脅威 2023」組織編

順位	組織に対する脅威
1位	ランサムウェアによる被害
2位	サプライチェーンの弱点を悪用した攻撃
3位	標的型攻撃による機密情報の窃取
…	…

IPA.「情報セキュリティ10大脅威 2023」.
https://www.ipa.go.jp/security/10threats/10threats2023.html,
(参照 2023-05-29)

HITACHI
Inspire the Next

主なインシデント事例

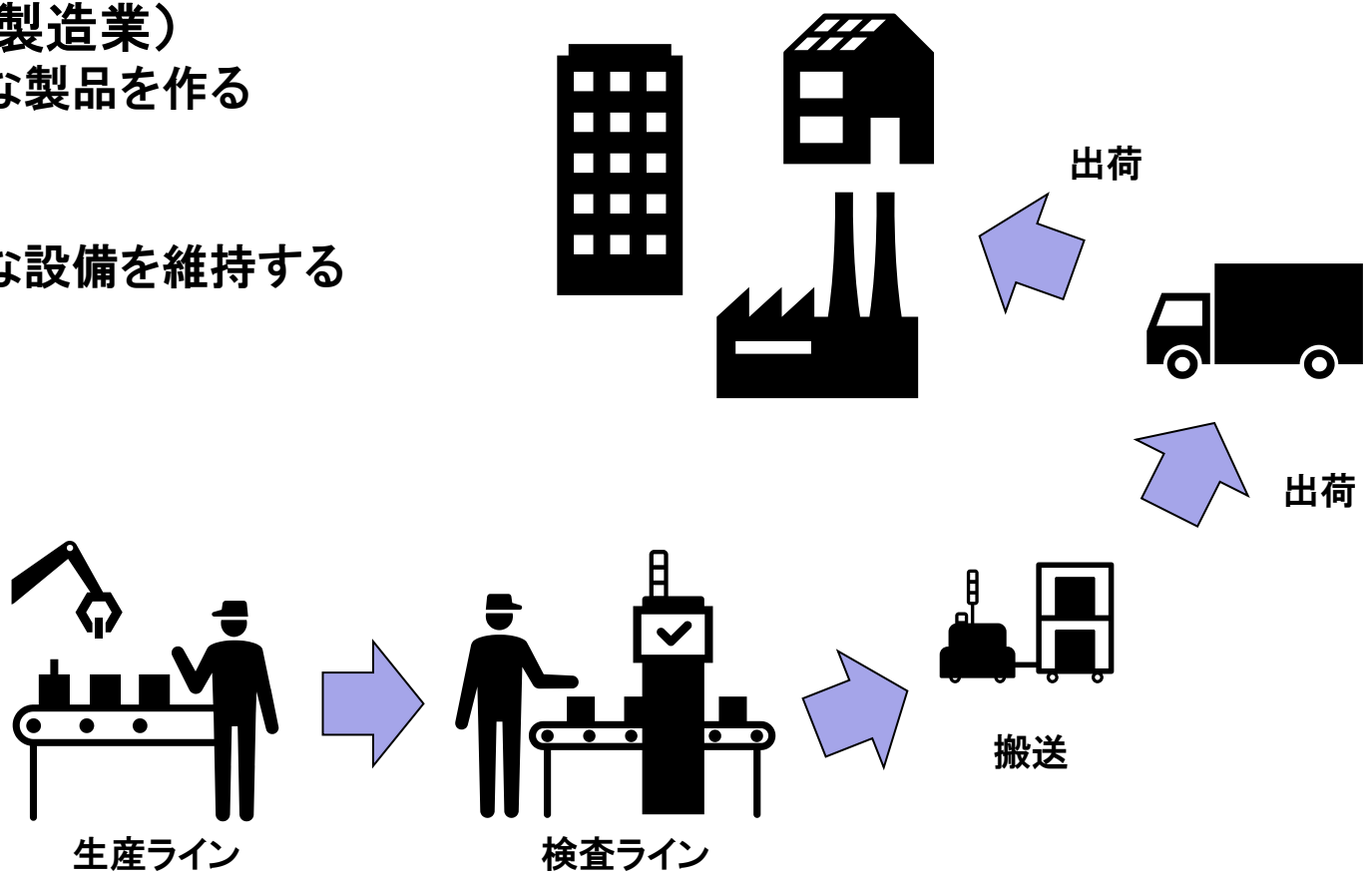
事例	報告時期	脆弱性のイメージ
■Log4shell Java言語のログ機能 ライブラリの脆弱性	2021年 11月	
■Ripple20 組み込み系機器に利用 される通信(TCP/IP) ライブラリの脆弱性	2020年 6月	

NEDO.「2021年度～2022年度成果報告書　戦略的イノベーション創造プログラム(SIP)第2期／IoT社会に対応したサイバー・フィジカル・セキュリティ/IoT社会に対応したサイバー・フィジカル・セキュリティに係るOSSの技術検証のあり方等に関する調査」. https://www.nedo.go.jp/content/100953488.pdf より事例を抜粋

1-3 工場におけるサプライチェーンセキュリティ

■製品の観点（製造業）
- セキュアな製品を作る

■設備の観点
- セキュアな設備を維持する

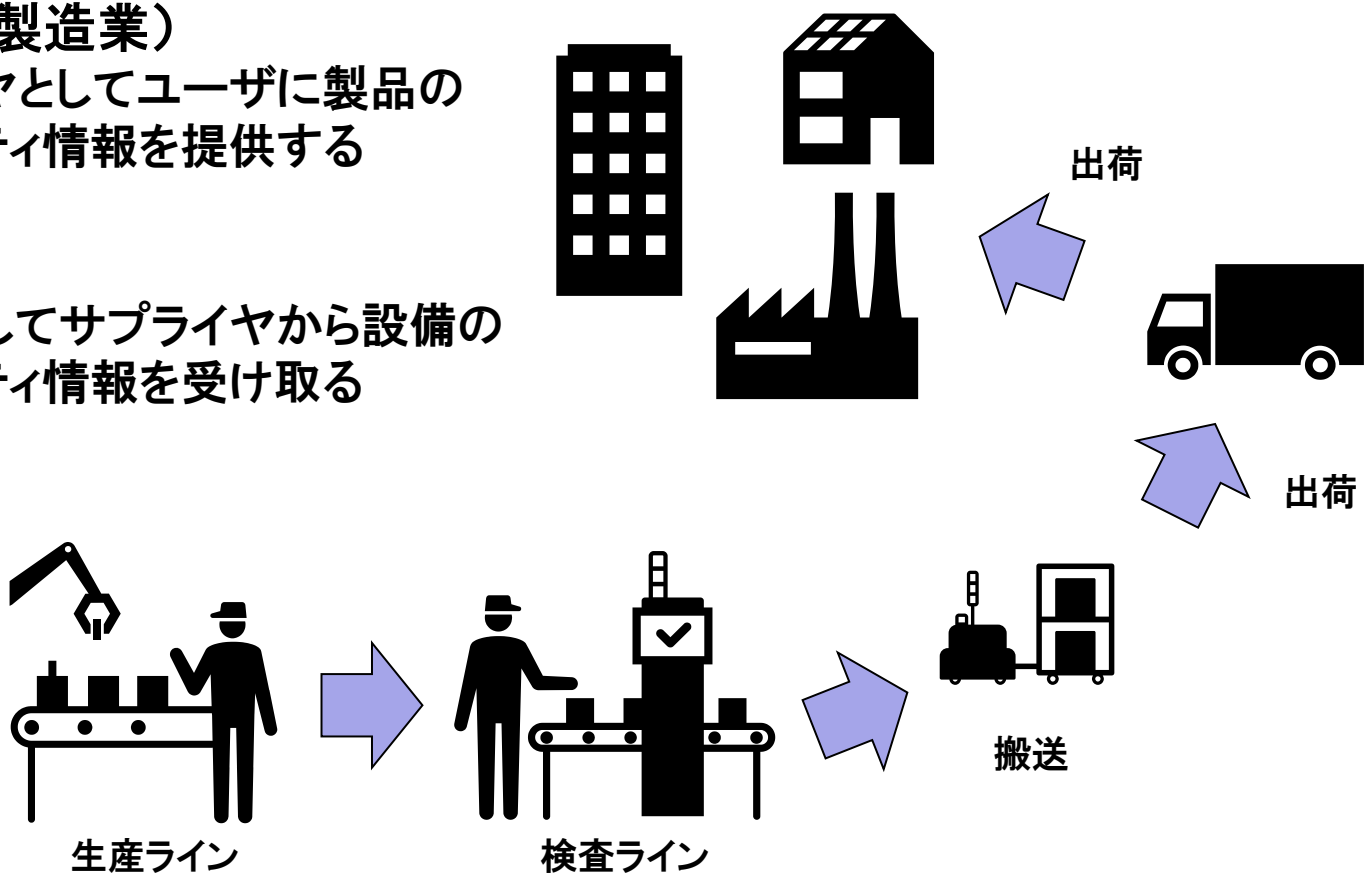


1-4 工場におけるサプライチェーンセキュリティ

HITACHI
Inspire the Next

■製品の観点（製造業）
- サプライヤとしてユーザに製品のセキュリティ情報を提供する

■設備の観点
- ユーザとしてサプライヤから設備のセキュリティ情報を受け取る



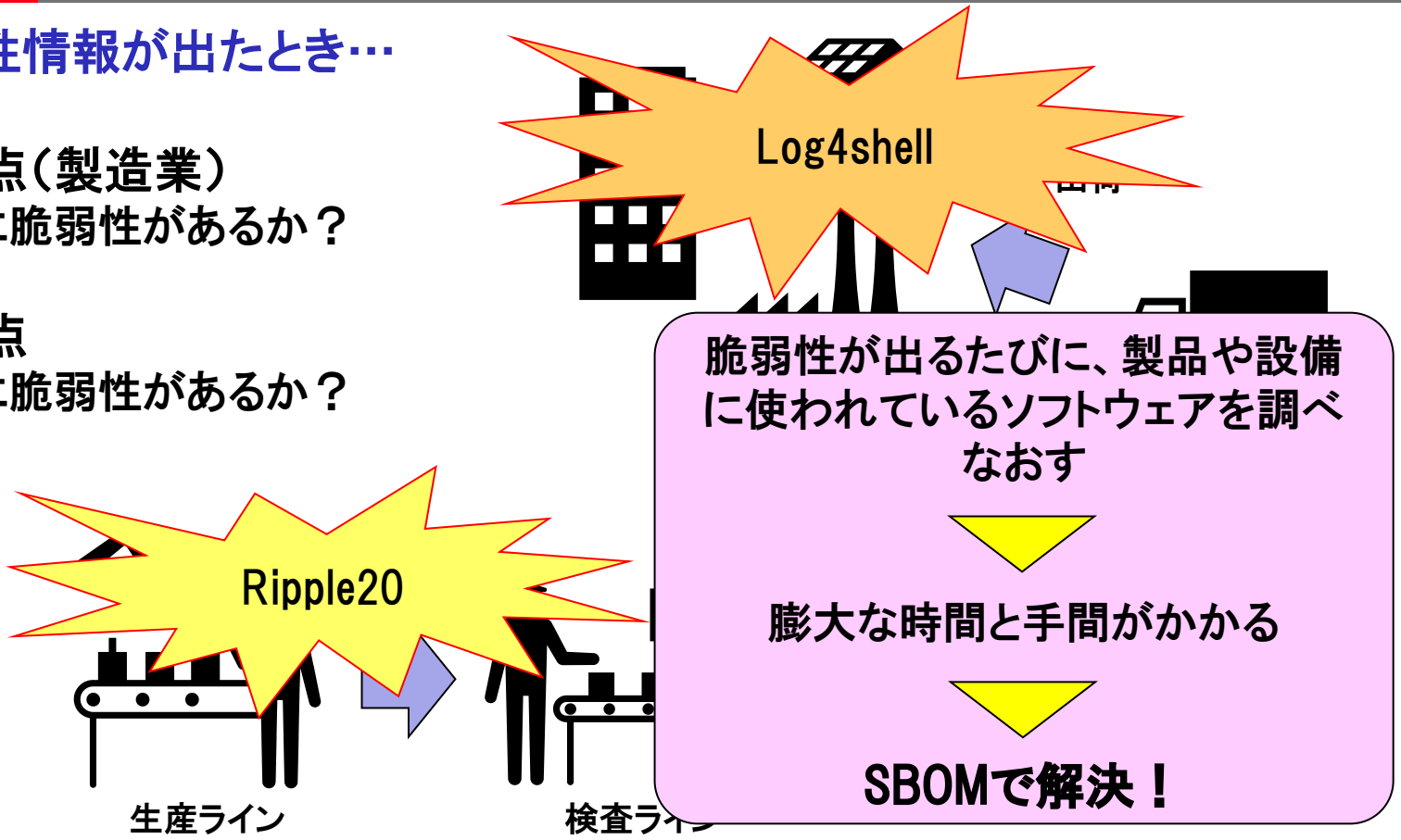
1-5 工場におけるサプライチェーンセキュリティ

HITACHI
Inspire the Next

大きな脆弱性情報が出たとき…

■製品の観点（製造業）
- 製品に脆弱性があるか？

■設備の観点
- 設備に脆弱性があるか？



脆弱性が出るたびに、製品や設備に使われているソフトウェアを調べなおす

▼

膨大な時間と手間がかかる

▼

SBOMで解決！

2. SBOM（Software Bill of Materials）とは

2-1 SBOM（Software Bill of Materials）とは

HITACHI
Inspire the Next

SBOM(ソフトウェア部品表)とは…

ある規則に従い機械が読める形をした、ソフトウェアコンポーネント、および依存関係やそれらに関する情報の一覧

基本情報
SBOMの作者
ソフトウェア(コンポーネント)の作成者
ソフトウェア(コンポーネント)の名前
ソフトウェア(コンポーネント)のバージョン
ソフトウェア(コンポーネント)のハッシュ値
ソフトウェア(コンポーネント)の識別子
ソフトウェア(コンポーネント)の関係性

NTIA.「SBOM at a Glance」(日本語訳). https://ntia.gov/sites/default/files/publications/sbom_at_a_glance_ja_0.pdf「Baseline Component情報」から意訳

HITACHI
Inspire the Next

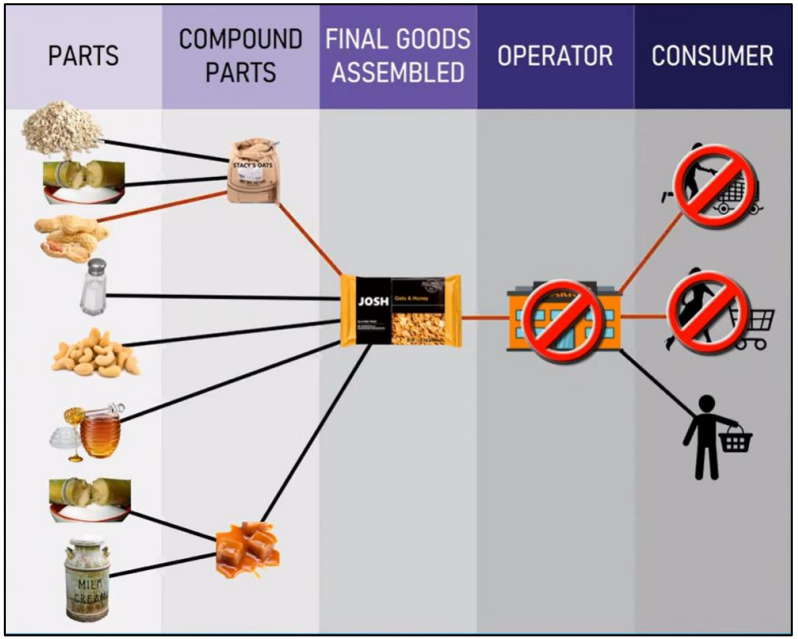
食品における食品成分表

・例えば、ピーナッツにアレルギーがある人がその製品を避けることができる

SBOMとしては

・特定のソフトウェアが入っている製品を避けることができる
・脆弱性のあるソフトウェアがあるかがすぐにわかる

部品　複合部品　製品　販社　消費者

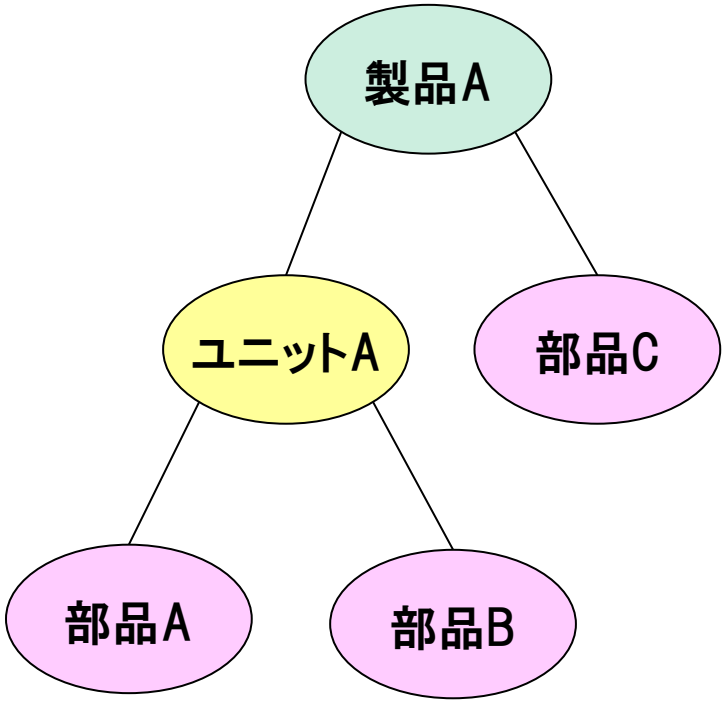


NTIA.「SBOM Explainer: What Is SBOM? Part 1」.
https://www.youtube.com/watch?v=6yljBKKI8Vo&list=PLO2IqCK7WyTDpVmcHsy6R2HWftFkUp6zG,
(参照 2023-05-29)

2-3 SBOMはBOMのソフトウェア版（SBOM ＝ ソフトウェアBOM）

HITACHI
Inspire the Next

BOM … 製品の構成要素や部品の一覧表。部品の調達や在庫管理などに用いられる。



BOM（製品A）	
品名	製品A
型式	
メーカ名	
材質	
…	

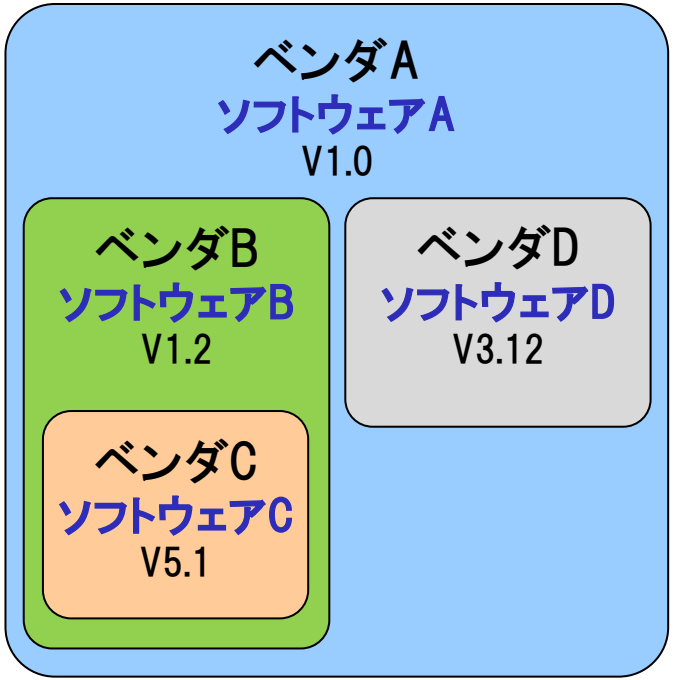
BOM（ユニットA）	
品名	ユニットA
型式	
メーカ名	
材質	
…	

BOM（部品A）	
品名	部品A
型式	…
メーカ名	…
材質	…
…	…

2-4 SBOMの簡単な例

HITACHI
Inspire the Next

ソフトウェア構成



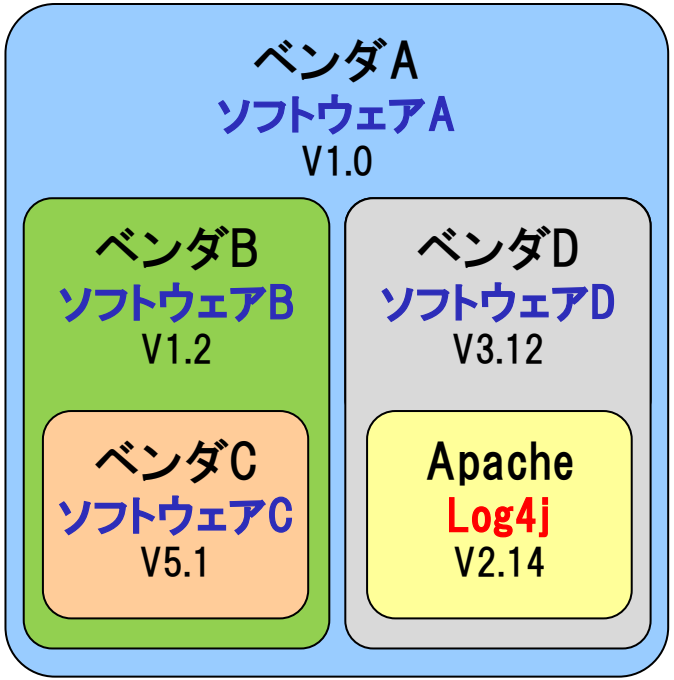
SBOM

作成者	ソフトウェア名	バージョン	…
ベンダA	ソフトウェアA	1.0	…
ベンダB	ソフトウェアB	1.2	…
ベンダC	ソフトウェアC	5.1	…
ベンダD	ソフトウェアD	3.12	…

2-4 SBOMの簡単な例

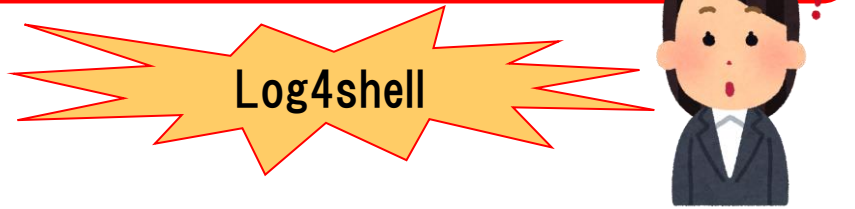
HITACHI
Inspire the Next

ソフトウェア構成



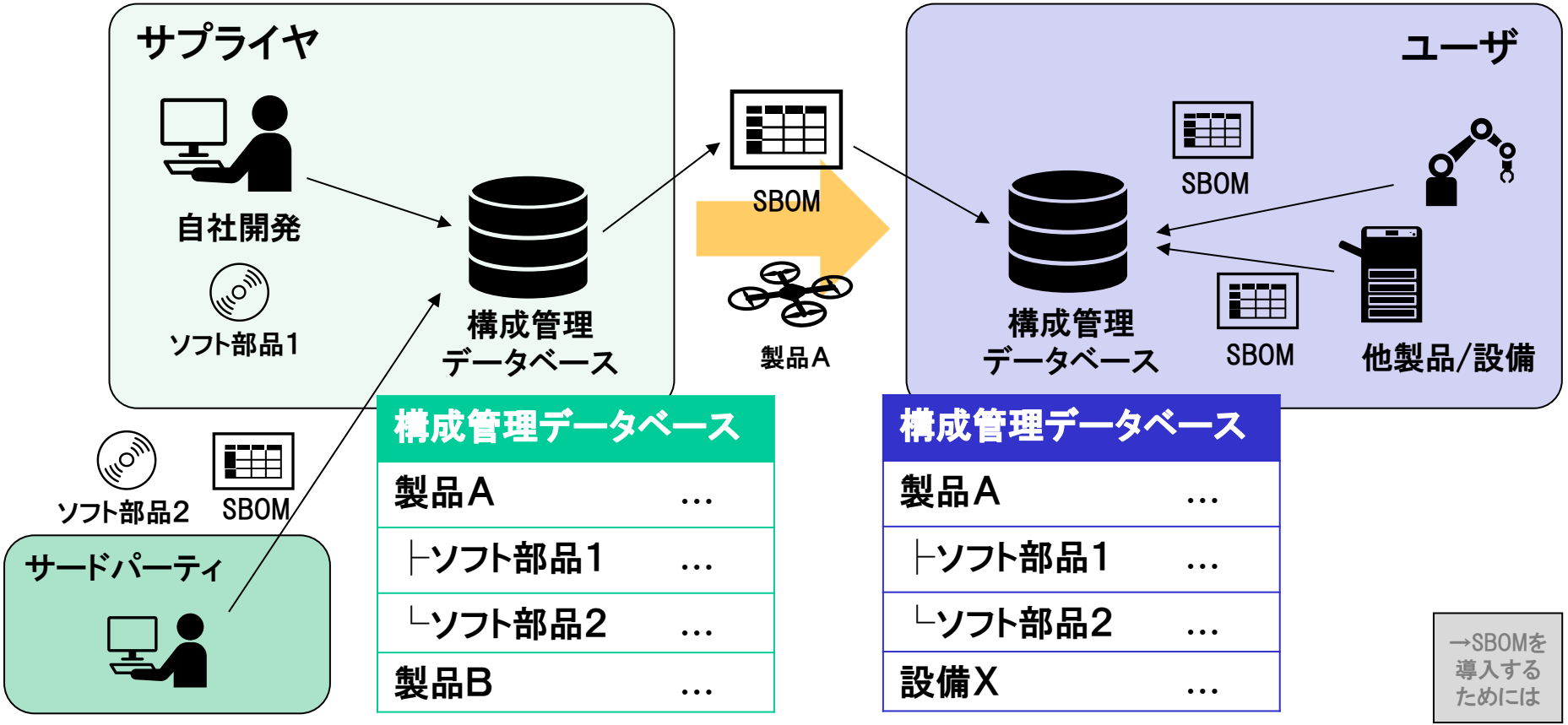
SBOM

作成者	ソフトウェア名	バージョン	…
ベンダA	ソフトウェアA	1.0	…
ベンダB	ソフトウェアB	1.2	…
ベンダC	ソフトウェアC	5.1	…
ベンダD	ソフトウェアD	3.12	…
Apache	Log4j	2.14	…



※Apache Log4jはLog4shellの脆弱性の対象となったソフトウェアコンポーネント

2-5 SBOMのエコシステム



2-6 SBOMの国際標準フォーマット

HITACHI
Inspire the Next

SBOMフォーマット種別	
SPDX https://spdx.dev/	➢ Linux Foundationによって取りまとめられた規格。 ➢ ソフトウェアライセンス情報のやり取りに主眼を置いている。
CycloneDX https://cyclonedx.org/	➢ OWASP Foundationによって取りまとめられた規格。 ➢ セキュリティ情報のやり取りに主眼を置いている。
SWID https://nvd.nist.gov/products/swid	➢ NISTによって取りまとめられた規格。 ➢ ソフトウェア資産管理に主眼を置いている。

HITACHI
Inspire the Next

3. SBOMを取り巻く状況

3－1 NTIA（アメリカ）

HITACHI
Inspire the Next

National Telecommunications and Information Administration

・米国商務省電気通信情報局
・2018年からソフトウェアコンポーネントの透明性について取り組む
➢ SBOMの啓発活動を行っており、ウェブサイトに活動レポートなどが公開されている

活動レポート（抜粋）	
2019年	➢ ヘルスケア業界でのPoC ➢ ユースケース：サプライチェーンにおけるSBOMの役割とメリット
2020年	➢ YouTubeでのSBOM解説（～2021年）
2021年	➢ 一目で分かるSBOM ➢ SBOMに関するFAQ ➢ 既存のSBOMフォーマットと標準に関する調査 …

NTIA.「SOFTWARE BILL OF MATERIALS」. https://ntia.gov/page/software-bill-materials より(参照 2023-05-29)

3－2 CISA（アメリカ）

HITACHI
Inspire the Next

Cybersecurity and Infrastructure Security Agency

・米国サイバーセキュリティインフラストラクチャセキュリティ庁
・国家のサイバーセキュリティとインフラストラクチャのセキュリティを管轄

➢ SBOMの啓発活動を行っており、ウェブサイトに活動レポートなどが公開されている。

活動レポート（抜粋）	
2022年	➢ VEX（Vulnerability Exploitability eXchange）ユースケース ➢ VEXステータス正当性
2023年	➢ SBOM共有化ライフサイクルに関するレポート ➢ SBOMのタイプについて ➢ VEXの最小要件

※VEX（Vulnerability Exploitability eXchange）は、脆弱性とその悪用可能性に関する情報を交換するための枠組み

CISA.「Software Bill of Materials (SBOM)」. https://www.cisa.gov/sbom より(参照 2023-05-31)

3－3 サイバー・レジリエンス法案（ヨーロッパ）

HITACHI
Inspire the Next

Cyber Resilience Act（2022年9月法案公開）

・ネットワークにつながるほとんど全てのデジタル製品にサイバーセキュリティ対策を義務化
・違反した場合の罰金は、1,500万ユーロ、もしくは年間総売り上げの2.5%の高いほう
・セキュリティの観点で、製品が備えるべき機能および製造業者の義務などを定めており、SBOMの作成も求められる

製造業者が満たすべき要件（付属書Ⅰの2）

1. 製品に含まれる脆弱性とコンポーネントを特定し、文書化すること。そのために機械読み取り可能な形式で一般的に使用されるSBOM作成（少なくとも最上位レベルの依存関係含む）を行うこと。
2. セキュリティアップデートの提供など、遅滞なく脆弱性に対処・緩和すること。
3. 効果的かつ定期的なテストとレビューを行うこと。

・・・

経済産業省サイバーセキュリティ課.「EUサイバーレジリエンス法（草案概要）」.https://www.jisa.or.jp/Portals/0/resource/news/1340/901.pdf より抜粋

HITACHI
Inspire the Next

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（2019年～）

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	
第7回（2022年7月）	➢ 医療機器、自動車、ソフトウェアの3つの分野でSBOM実証を進める ➢ SBOMに関するノウハウ集、活用モデル、取引モデルを作成する
第8回（2022年11月）	➢ 実証でこれまで確認された課題の共有 • ツールを適用しただけでは特定されないケースが多数存在 • 異なるSBOMツール間でのSBOMの共有が困難
第9回（2023年2月）	➢ 初級者向けSBOM導入手引 ➢ 導入手引、対応モデル、取引モデルの意見公募→普及・啓発（2023/2024年度）

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」.
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/index.html
各回のレポート「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」より抜粋

3－5 厚生労働省（日本）

HITACHI
Inspire the Next

医療機器のサイバーセキュリティ導入に関する手引書（第2版）（2023年3月）

➢ 製造業者向け

顧客向けセキュリティ文書	
例	➢ 医療機器製品に実装されている自製、OSS及び市販のソフトウェア部品の透明性を確保するためのSBOM

※OSS … Open Source Software。ソースコードが公開されており、ソースコードの使用や修正、再配布などが可能なソフトウェアの総称。

厚生労働省.「医療機器のサイバーセキュリティ導入に関する手引書の改訂について」. https://www.mhlw.go.jp/hourei/doc/tsuchi/T230404I0050.pdf より抜粋

医療機関における医療機器のサイバーセキュリティ確保のための手引書（2023年3月）

➢ 医療機関向け

医療機器の導入時	
医療機器業者から提供される情報の例	➢ 医療機器に実装されているソフトウェアに関する情報を含むSBOM。SBOMは、販売時及び変更があった場合に提供される。

インシデントへの対応	
対応策の実行	➢ SBOM、脆弱性・アップデートなどの情報、医療セプター等からの情報を受領し、広く共有すること。

厚生労働省.「医療機関における医療機器のサイバーセキュリティ確保のための手引書について」. https://www.mhlw.go.jp/hourei/doc/tsuchi/T230404G0080.pdf より抜粋

HITACHI
Inspire the Next

4. SBOMの導入

4-1 SBOMを導入するためには

HITACHI
Inspire the Next

SBOMを定義し、運用に関して取り決めを行い、運用する

	内容例
SBOMの定義	➢ サプライチェーンで共有できるよう、自社独自フォーマットではなく、標準化されたフォーマットを使う(SPDX、CycloneDX、SWID)。
SBOMの運用に関する取り決め	➢ SBOMを作成/更新するタイミングを取り決め、既存のプロセスに組み込む。 ➢ SBOMを下流企業に提供する方法を定義する。(必要に応じて機密性、完全性を担保)
SBOMの運用	➢ 上流企業に対して、SBOMの提供を要求する。 ➢ 自動化を計画、実施することが望ましい。
段階的な対応	➢ 手動管理→自動管理、自社内管理→サプライチェーン連携 という段階的な対応を検討。

NEDO.「2022年度成果報告書　戦略的イノベーション創造プログラム(SIP)第2期／IoT社会に対応したサイバー・フィジカル・セキュリティ／IoT社会に対応したサイバー・フィジカル・セキュリティに係るOSSの管理手法及びCSIRT・PSIRT連携等に関する調査」. https://www.nedo.go.jp/content/100956036.pdf より抜粋

→SBOMのエコシステム

本日の振り返り

HITACHI
Inspire the Next

- SBOMとは
  - ✓ SBOMとは
- 欧米において、SBOM導入に向けた活動が活発、立法化が進んでいる
  - ✓ NTIA/CISA、EUサイバーレジリエンス法案
- 日本においてもSBOM導入に向けて検討が進んでいる
  - ✓ 経済産業省、厚生労働省
- 部分的、段階的にでもSBOMの導入を進めていきましょう
  - ✓ SBOMを導入するためには

HITACHI
Inspire the Next

END

サプライチェーンを可視化するSBOMとは

2023/06/09

日立チャネルソリューションズ株式会社
コア技術開発センタ　ソリューション技術開発本部　ソリューション技術開発部／技師

一般社団法人　重要生活機器連携セキュリティ協議会（CCDS）
研究開発センター／シニアリサーチャー

石川智祥

参考資料

資料1 FS-ISAC（Financial Services Information Sharing and Analysis Center）

HITACHI
Inspire the Next

米国を中心としたグローバルの金融機関や関連企業が参加する、セキュリティに関する情報や脅威の共有を行う共助組織。

- 【2015年10月】「Appropriate Software Security Control Types for Third-Party Service and Product Providers」

BOM (SBOM) のユースケース	
一次的なもの	➢ 脆弱性データベースと照らし合わせて、既知の脆弱性を洗い出す
二次的なもの	➢ データの変換を必要とせず、集中管理可能 ➢ ソフトウェアのリスクスコアリング ➢ 脆弱性管理における優先順位付け ➢ 知的財産に関する課題の認識 …

FS-ISAC.「Appropriate Software Security Control Types for Third-Party Service and Product Providers」.
https://www.fsisac.com/hubfs/Resources/FSISAC-ThirdPartySecurityControlTypes-Whitepaper_2015.pdf より抜粋

HITACHI
Inspire the Next

米国大統領令14028。米国国家のサイバーセキュリティの向上に関して、脅威情報の共有やソフトウェアサプライチェーンセキュリティ強化などを指示。（2021年5月）

・ソフトウェアサプライチェーンセキュリティ強化（セクション4）では、NTIAに対してSBOMの最小要素をまとめるように指示。⇒ これを受けてNTIAがリリース（2021年7月）

SBOMの最小要素（Minimum Elements for a SBOM）	
データフィールド	➢ どのような情報を記録する必要があるか
自動化のサポート	➢ ソフトウェアエコシステムで広く適用していくためには自動化が必須
実践とプロセス	➢ SBOMをいつ作成するかなどの運用を定義

NTIA.「The Minimum Elements For a Software Bill of Materials (SBOM)」. https://www.ntia.doc.gov/report/2021/minimum-elements-software-bill-materials-sbom で公開された資料より作成

資料3 NIST（National Institute of Standards and Technology）

HITACHI
Inspire the Next

米国国立標準技術研究所。科学技術と技術標準の発展を支援するために設立。
サイバーセキュリティを含む、幅広い技術領域にわたる基準とガイドラインを開発。

・【2022年5月】「Software Supply Chain Security Guidance」大統領令14028を受けたソフトウェアサプライチェーンのセキュリティに関するガイダンス。SBOMに関するものも含む。

推奨されるSBOM能力	
基礎的能力	➢ 業界標準のフォーマットを採用。NTIAの最小要素を満たす。など
持続的能力	➢ 取得側のリスク状況に関する追加情報を含める。SBOMリポジトリに脆弱性検出機能を統合する。など
発展的能力	➢ SBOMのベンダ提供がない場合にバイナリ解析してSBOMを生成する。など

NIST.「Software Security in Supply Chains: Software Bill of Materials (SBOM)」. https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains-software-1 より作成

資料4 OpenChain（ISO/IEC 5230）

HITACHI
Inspire the Next

OSS(Open Source Software)ライセンスコンプライアンスの確立を目指す、Linux Foundationのプロジェクトの1つ。OpenChain 2.1はISO/IEC 5230:2020として国際規格化(2020年12月)。

項目例	内容例
プログラムにおける基本事項	ソフトウェアのライセンス遵守を管理するポリシーが必要。書面化し社内に周知する。
関連タスクの定義とサポート	プログラム実行には責任、時間・予算が必要。ポリシーのレビューや更新、サポートプロセスを整備する必要がある。
OSSコンテンツのレビュー及び承認	SBOMを作成・管理するプロセスが必要。提供するソフトウェアの各OSSコンポーネント(およびそのライセンス)を含む。
コンプライアンス成果物の生成と配布	提供するソフトウェアについての一連のコンプライアンス成果物を作成するプロセスが存在すること。
OSSコミュニティへの貢献	OSSプロジェクトへの貢献を考慮する場合、ポリシーを文書化し、内部に伝達し、実施するためのプロセスを整備する必要がある。

The OpenChain Project.「OpenChain Specification Version 2.1」. https://github.com/OpenChain-Project/License-Compliance-Specification/blob/master/2.1/en/openchainspec-2.1.pdf より作成

資料5 Payment Card Industry (PCI)

HITACHI
Inspire the Next

国際カードブランドによって設立されたPayment Card Industry Security Standards Council (PCI SSC)が策定する、クレジットカードデータを保護するためのセキュリティ基準群。
「Secure Software Standard」は、クレジットカードを扱うソフトウェアを対象とする認証規格。

・【2022年12月】Secure Software Requirements and Assessment Procedures Version 1.2 をリリース。Web上で動作するソフトウェアを対象とした要件にSBOMが追加。

Webソフトウェアを対象とした、SBOMに関する要件(抜粋)	
C.1.1	➢ すべてのソフトウェアコンポーネントとサービスを文書化、もしくはソフトウェア部品表(SBOM)の形でカタログ化すること。
C.1.2	➢ SBOM には使用中している一次的なコンポーネントとサービスを記述すること。さ らにそれらの二次的なコンポーネントに対する関係や依存関係を可能な限り記述すること。
…	➢ …

NEDO.「2022年度成果報告書 戦略的イノベーション創造プログラム(SIP)第2期／IoT社会に対応したサイバー・フィジカル・セキュリティ／IoT社会に対応したサイバー・フィジカル・セキュリティに係るOSSの管理手法及びCSIRT・PSIRT連携等に関する調査」. https://www.nedo.go.jp/content/100956036.pdf より抜粋

資料6 トヨタ自動車の例

HITACHI
Inspire the Next

- サプライチェーン全体に渡ってOSSのコンプライアンスを実現する業界標準「OpenChain」の活動

- 各サプライヤと使用ソフトウェアに関するガイドラインを合意
  - サプライチェーンにおけるOSS コンプライアンスの役割、使用ソフトウェアリスト(SBOM)を提供すること など

- 部品供給に際して、自社と各サプライヤのエンジニア部門同士で使用ソフトウェア報告の運用規則について合意
  - 規則の適用範囲、SBOMの報告方法、報告のタイミング など

経済産業省.「OSSの利活用及びそのセキュリティ確保に向けた管理手法に関する事例集」. https://www.meti.go.jp/press/2022/05/20220510001/20220510001-1-2.pdf
経済産業省.「第3回 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」→「OpenChain Projectにおける OSSのTransparency向上への取組」. https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/003_04_00.pdf より抜粋