【座学】05

世界で脅威が認識されつつある「製品のセキュリティ」とは？

2025/11/20

はじめに

本日は、少し前から話題に挙がっているものの、絶対的な情報量が多くないこともあって、ITやセキュリティの世界ではそれほど取り扱われることが多くない「製品セキュリティ」のお話しをしたいと思います。

正直、InternetWeek2025のコンテンツとしては、あまりそぐわず、不人気かなと思っていたのですが、意外にもたくさんのお申込みがありました。本講演の企画者として非常に嬉しい限りです。

まず

本当に、製品セキュリティは「世界で脅威が認識されつつある」のか？

残念ながら答えは

YES です。

実際に米国とEUでは、製品セキュリティの法整備が急速に進んでいます。

米国では

米国大統領令 14028号
「サイバーセキュリティの改善」
（2021/5/12 発令）

違反した場合

政府調達品から除外される。

EUでは

欧州サイバーレジリエンス法/CRA
（2024/12/10施行）

違反した場合、❶or❷の高い方の罰金

❶1500万€（26.5億円）
❷全世界年間売上の2.5％

このような法整備が進んでいる理由は、主に以下の2点です。

ソフトウェアの脆弱性

スパイウェア

本日の登壇者

日本ネットワークセキュリティ協会 IoT Security WG リーダ
➡某OSメーカーの組込みエンジニア

重要生活機器連携セキュリティ協議会 フェロー
元JPNIC 理事
➡元メーカーのエンジニア

日本シーサート協議会 運営委員
➡ガンダムのセキュリティ記事とか書いている人
（企画者兼モデレーター）

製造業の2026年の最大の課題：CRA対応

CRAの最終期限は、以下の主要な義務の適用開始日（2027年12月11日）です。この適用期日までにCRAへの準拠を達成し、CEマーキングを取得する必要があります。もし、この措置を怠った場合は 製品のEU市場への投入が禁止されます。また、2026年9月11日の「脆弱性およびインシデント報告義務の適用開始日」も重要です。この日までに**社内の体制を整備し、脆弱性とインシデント発生時の報告義務を果たせる**ようにしなければなりません。

2024年12月10日	CRA（サイバーレジリエンス法）の施行日 済
2026年6月11日	適合性評価機関に関する要件の適用開始日
重要 2026年9月11日	脆弱性およびインシデント報告義務の適用開始日
重要 2027年12月11日	主要な義務の適用開始日

CRAの対象外になる製品

CRAの対象はほとんどの「デジタル製品」です。その具体的な定義は「ソフトウェアまたはハードウェア製品およびそのリモートコンピューティングソリューションであって、個別に市場に投入されるものも含む」というものです。
なお、CRA対象外となる製品（やサービス）もいくつかあり、以下を明確に「規制対象外」としています。ただし、対応しなくてよいというよりCRAとは別の枠組み対応するため、重複を避けて対象外としているものが多いです。

CRA非対称製品

❶ 医療機器規則（EU 2017/745）の対象となる医療機器
❷ 体外診断用医療機器規則（EU 2017/746）の対象となる医療機器
❸ 国家安全保障や防衛機器（軍事用途等）
❹ 民間航空機規則（EU 2018/2139）の対象となる航空機関連機器
❺ 自動車の型式承認規則（EU 2019/2144）の対象となる自動車関連機器
❻ SaaS（Software as a Service）
❼ 非営利目的のオープンソースソフトウェア（OSS）

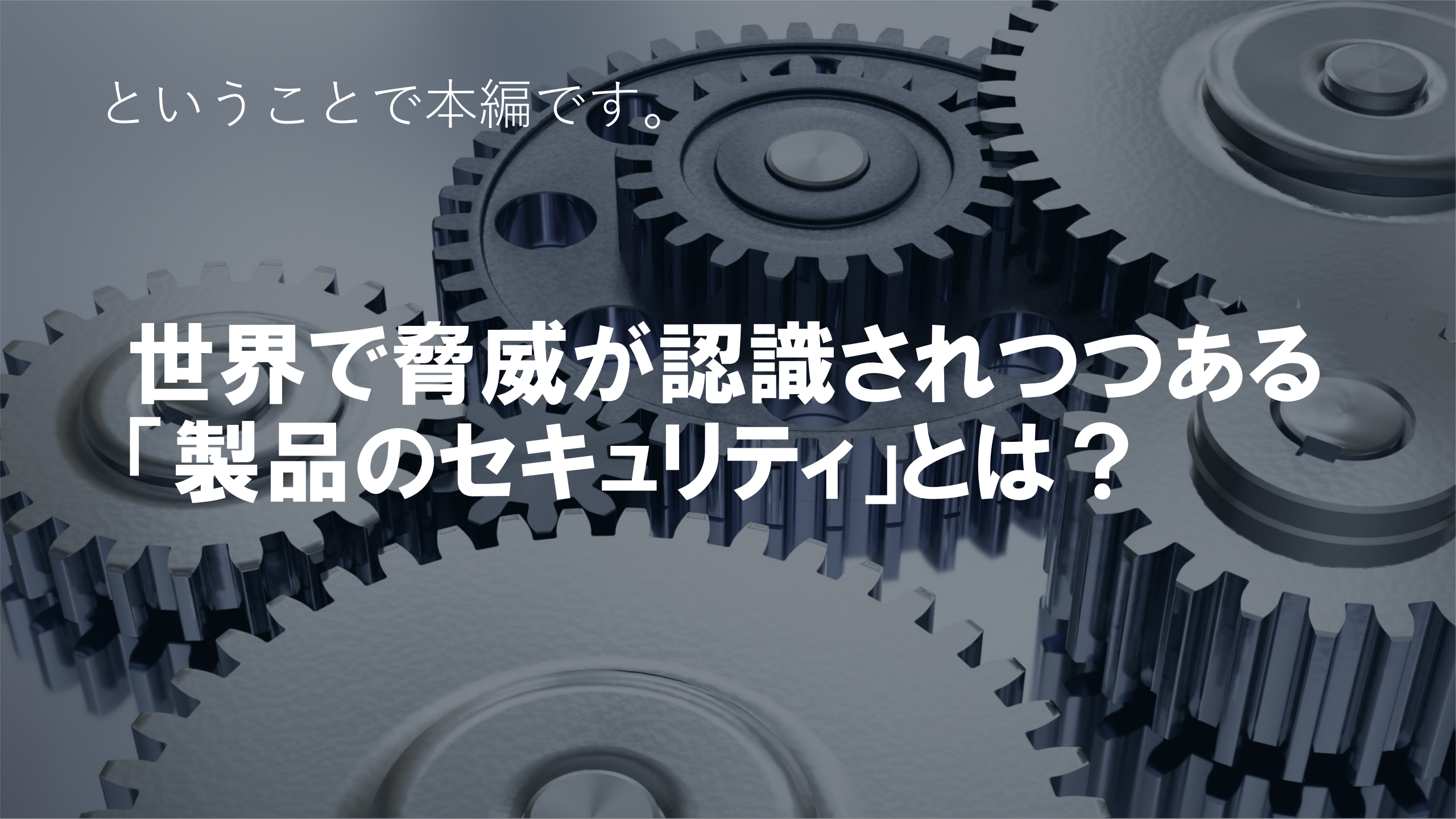
日本の製造業は、これらの対象となるデジタル機器を製造しています。また、米国や欧州への輸出企業はほとんどの場合で対応が必須となります。特に、CRA対応は期限も近く迅速な対応が必要！

なので、「製品のセキュリティ」への対応がどんどん進んでいくと考えていたのですが、なんか順調に進んでいく感が無いのです。

なので、ちょっと考えました！

たぶん、「デジタル製品」製造企業やその会社にいる人たち、そして市場の啓発が進んでいないんだと考えまして・・・

今回の講演を企画しました！



ということで本編です。

世界で脅威が認識されつつある「製品のセキュリティ」とは？

ということで、この分野に詳しい人に「CRA」「SBOM」など製品セキュリティについてディスカッションします。

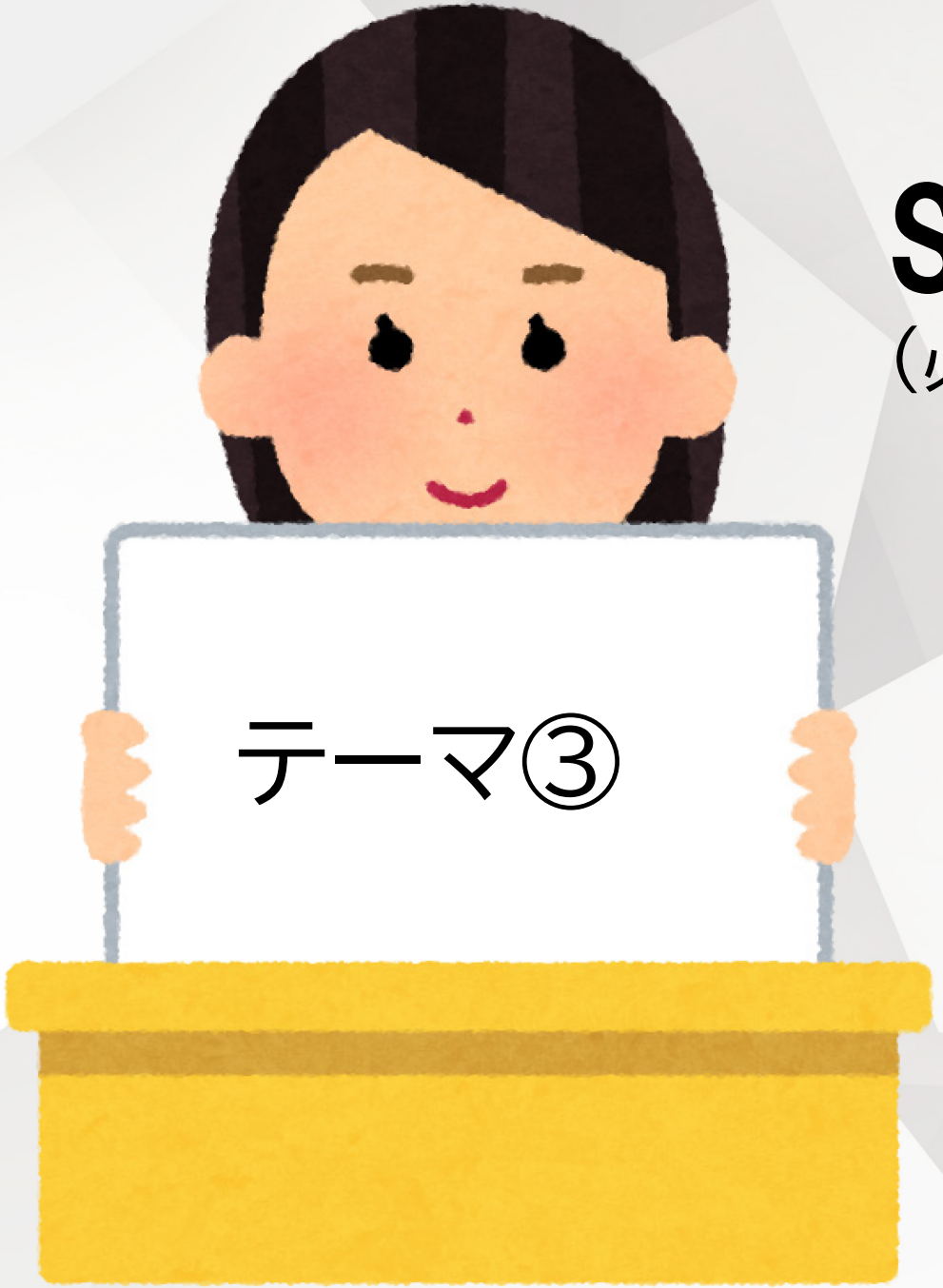
と言っても、難しい
話には極力しない
予定なので
こんな感覚で聴いて
頂ければと思います。

製品のセキュリティとはそもそも何か？

（ITのセキュリティとの違い等）

米国大統領令や欧州のCRAはどのような経緯や背景で制定された？

（米国やEU各国政府は何がしたい？）



SBOMとは何ですか？

（必要な理由、情シスでの活用の是非等）

SBOMに関する補足

（Google GEMINI2.5）

SBOM（Software Bill of Materials）とは、ソフトウェアの構成要素とその依存関係をリスト化したもので、日本語では「ソフトウェア部品表」と訳されます。簡単に言うと、ソフトウェアがどのような部品（コンポーネント）で構成されているか、各コンポーネントのバージョンやライセンス、そしてそれらの間の関係性をまとめたものです。

SBOMの主な目的は、ソフトウェアのサプライチェーンにおける透明性を高め、セキュリティリスクを特定・管理しやすくすることです。ソフトウェア開発における部品（コンポーネント）が脆弱性を抱えていたり、不適切なライセンスで使われていたりする場合、それがサプライチェーン全体に影響を与える可能性があります。SBOMによってこれらのリスクを可視化し、早期に発見・対応できるようになります。

なぜ、デジタル製品に脆弱性やスパイウェアが混入してしまうのか？

なぜ、デジタル製品に多くのOSSが活用されているのか？

（OSSが問題なら使わなければ良い理論）

フリーディスカッション

ディスカッションテーマ終了

（次頁はAppendix/SBOMアンケート調査）

Appendix

アンケート調査

日本における「SBOMの現状」はどのようになっているのか？

※株式会社ベリサーブ調べ

製造業の「設計・開発部門」「品質管理部門」の1,000名の方に

アンケートを実施してみました！

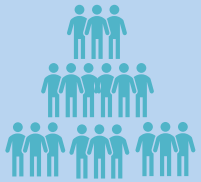
市場調査の調査対象について

製造 業設計開発/品質管理部門担当者1,000人、webアンケートツール「QiQUMO」に登録されているパネリストの中から、下記の条件に該当する12,252名に事前スクリーニング調査を実施し抽出しました。

事前スクリーニング調査対象

＜業種＞

- ✅ 電器・機械・輸送用機器
- ✅ 半導体・精密機器・コンピューター・通信機器
- ✅ 家電製品
- ✅ 自動車
- ✅ その他製造業



12,252人

本調査対象

＜事前スクリーニング調査での回答＞

- ✅ 設計開発部門
- ✅ 品質管理部門

2,599人

1,000人
分の回答を回収

調査対象

製造業の設計開発部門で働く担当者1,000名
・品質管理部門：324名（32.4%）
・設計開発部門：676名（67.6%）

調査時期

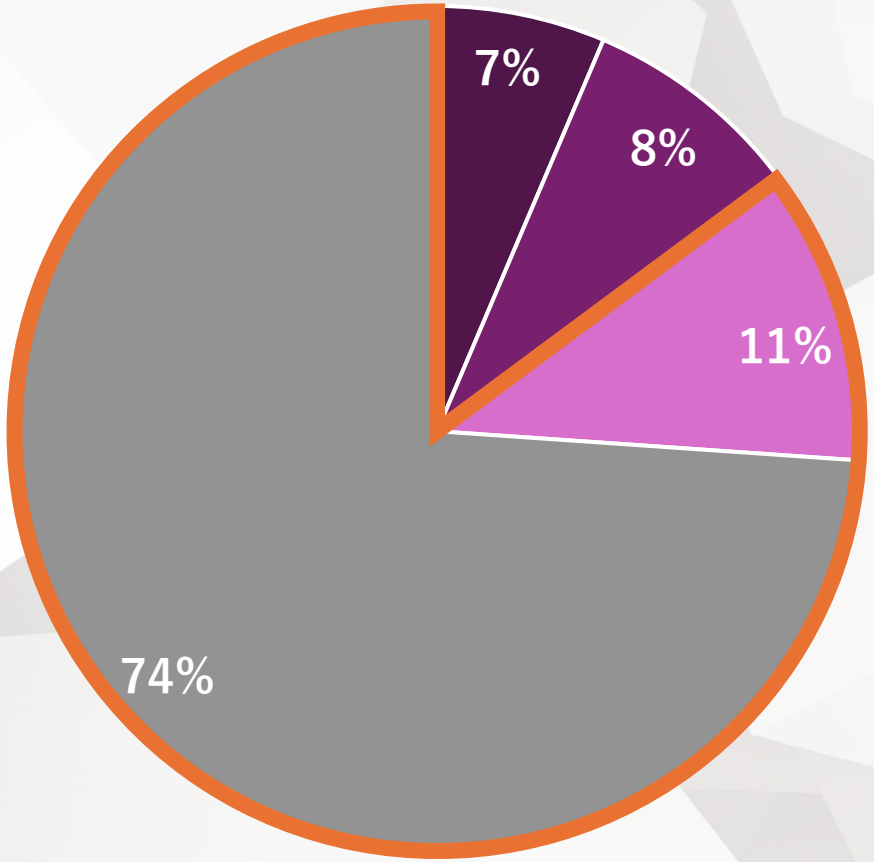
2025年5月

調査手法

オンラインアンケート

SBOM市場調査アンケート

Q1　SBOMについてご存じですか？



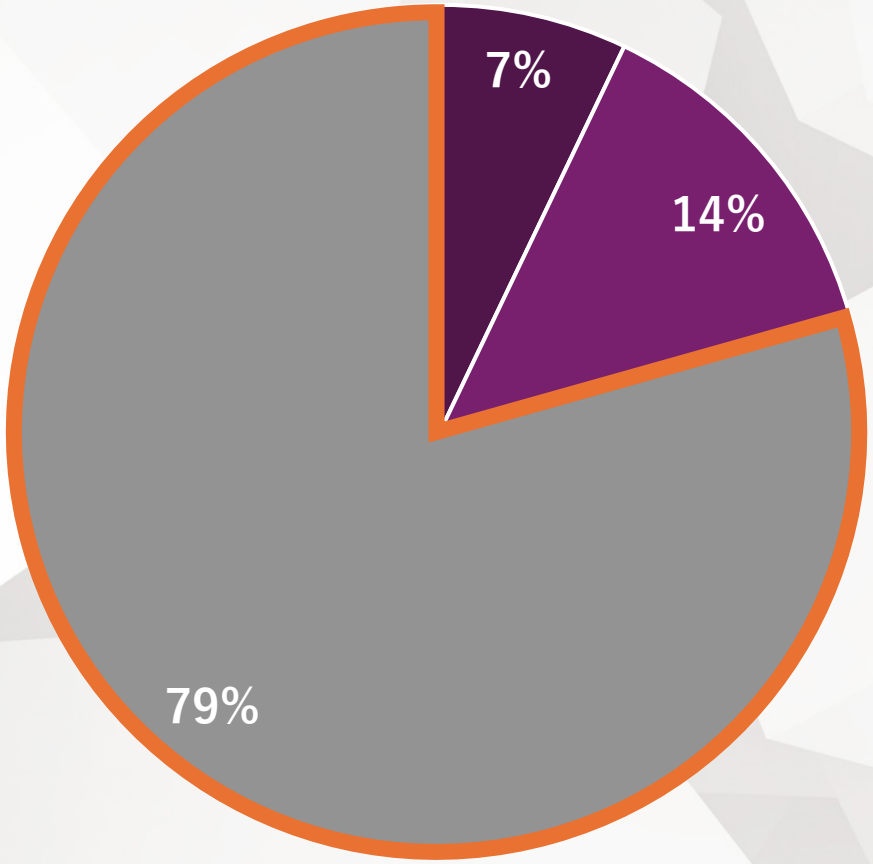
回答選択肢	回答人数
調査を終え、詳しく理解している	64
調査中で概要を理解している	84
聞いたことはある	113
知らない	739

85%

がSBOMを把握していない

SBOM市場調査アンケート

Q2　SBOM導入状況についてお聞かせください。



回答選択肢	回答人数
導入済	71
導入検討中	136
導入予定はない	793

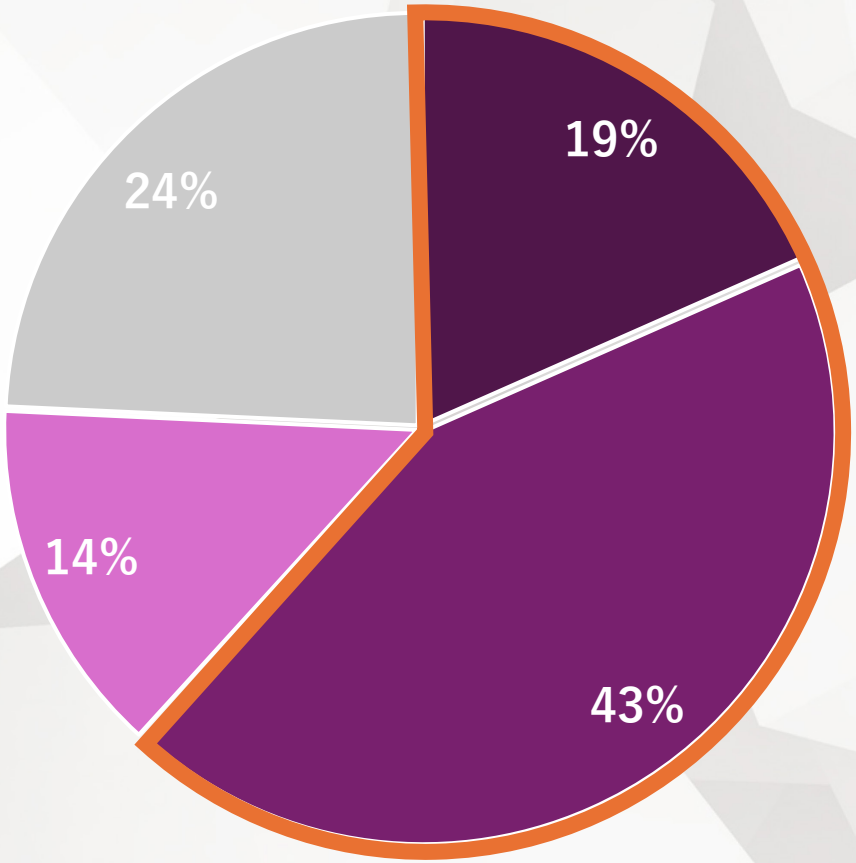
導入済は7%にとどまり

79%

が導入予定なし

SBOM市場調査アンケート

Q3　いつ頃の導入を検討していますか？ ※Q2で「導入検討中」と回答した方（136名）のみ



※ただし、全体数での割合は8.4%（84名）にとどまる

回答選択肢	回答人数
2026年3月まで	25
2026年9月まで	59
2026年10月以降	19
未定	33

「導入検討中」と回答した方の

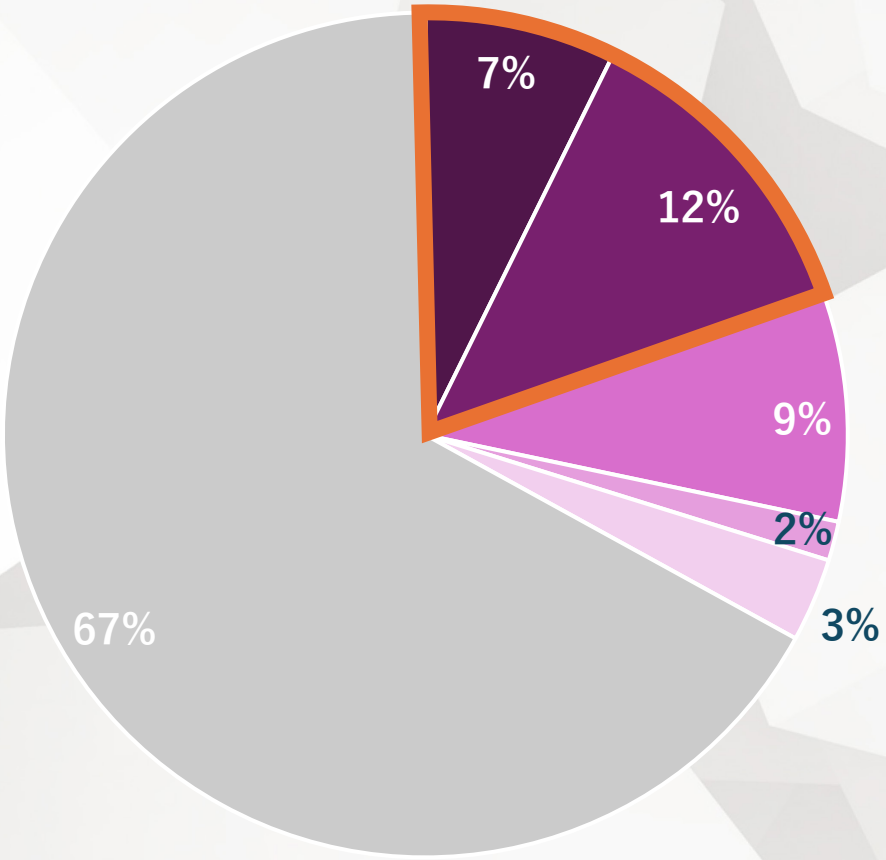
62%

が2026/9までの導入検討

※ 2026/9は脆弱性およびインシデント報告義務の適用開始日です。

SBOM市場調査アンケート

Q4　SBOMが脆弱性管理においてどれほど重要だと考えていますか？



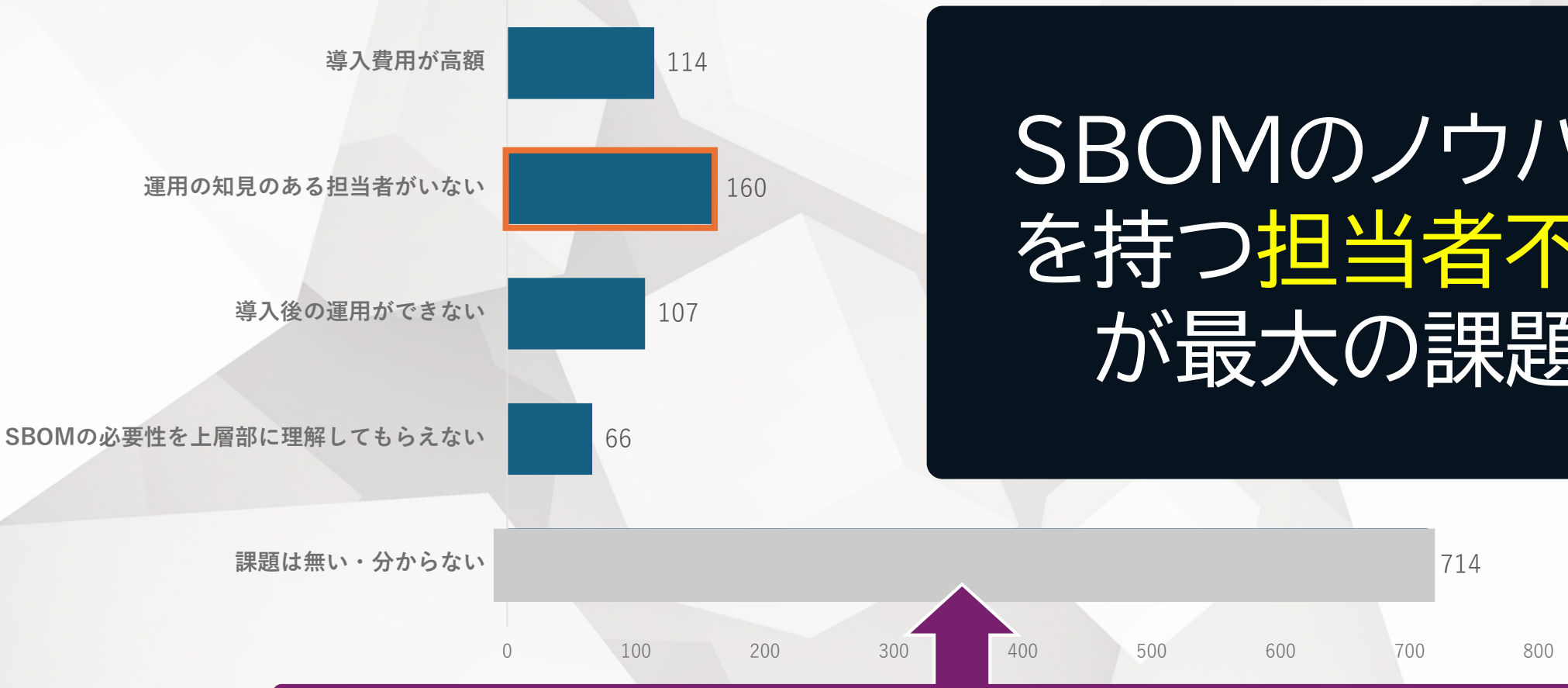
回答選択肢	回答人数
とても重要（SBOM導入済または導入予定）	73
重要（他の代替手段含めて検討している）	123
ふつう（無いよりあった方が良いという程度）	87
あまり重要でない	15
まったく重要ではない	32
分からない	670

19%

だけがSBOMを重要と回答

SBOM市場調査アンケート

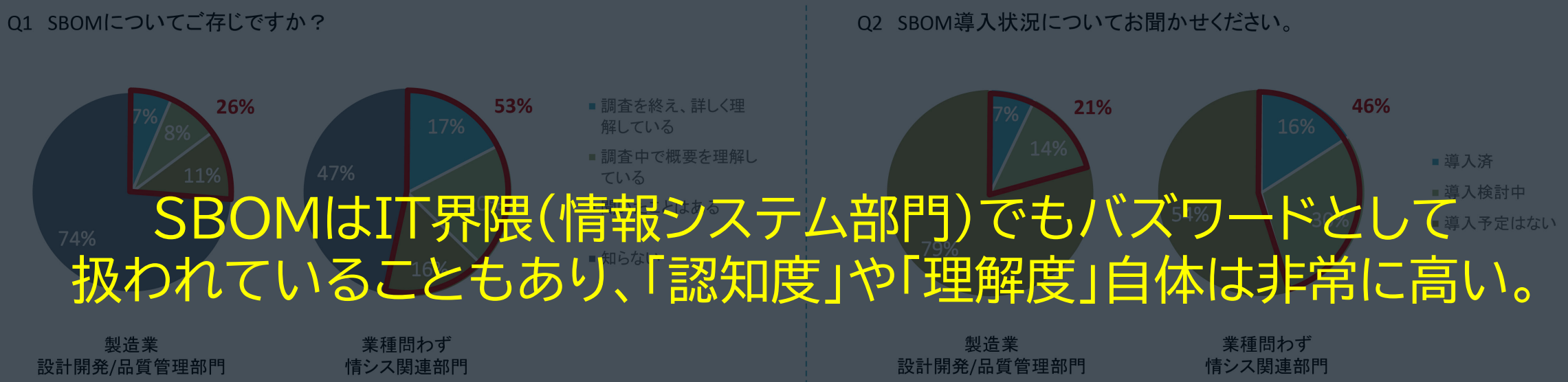
Q5　SBOMを導入するにあたり、どのような障壁や課題を感じていますか？（複数回答可）



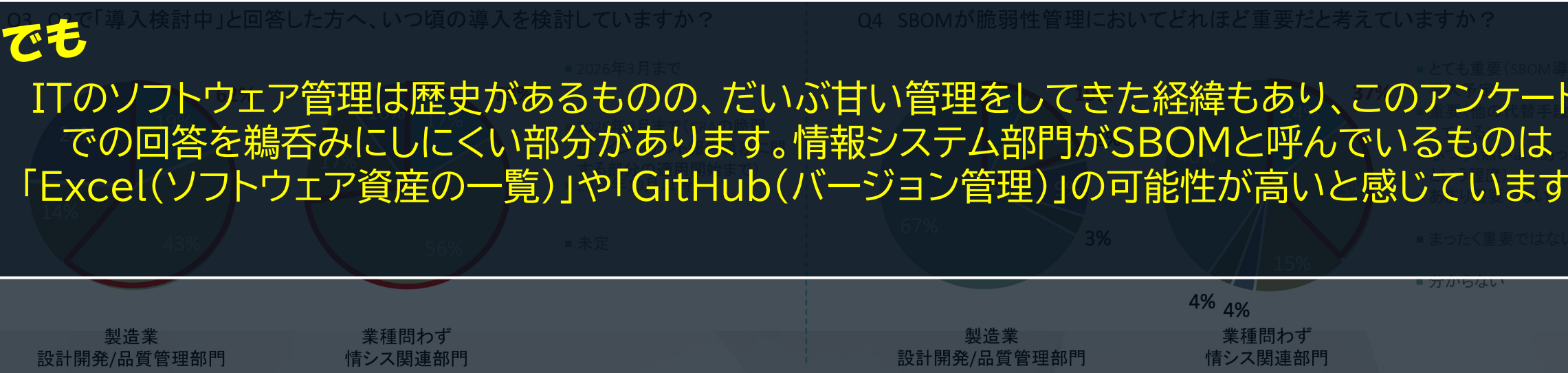
SBOMのノウハウを持つ担当者不在が最大の課題

でも、本当の課題はそもそも「課題がわからない」こと…かも？

参考：情報システム部門への調査との比較



SBOMはIT界隈（情報システム部門）でもバズワードとして扱われていることもあり、「認知度」や「理解度」自体は非常に高い。



でも

ITのソフトウェア管理は歴史があるものの、だいぶ甘い管理をしてきた経緯もあり、このアンケートでの回答を鵜呑みにしにくい部分があります。情報システム部門がSBOMと呼んでいるものは「Excel（ソフトウェア資産の一覧）」や「GitHub（バージョン管理）」の可能性が高いと感じています。

まとめ

製造業の設計開発・品質管理部門における

SBOM認知度は低く、まだ15%程度

「脆弱性およびインシデント報告義務の適用開始日（2026/9）」までの対応予定は84/1,000件に過ぎず

CRA対応も実施企業はまだ限定的

CRAを理解していれば、当然SBOM構築・運用が必須となることに辿り着くはずだが…

CRA対応とSBOMの関係性への理解も不足

ご清聴ありがとうございました。