経済産業省

資料3

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

令和４年７月26日

経済産業省　商務情報政策局

サイバーセキュリティ課

1. 昨年度のタスクフォースにおける議論の振り返り

2. ソフトウェアの管理手法等に関する国外の状況

3. 令和4年度のSBOM実証イメージ

4. ノウハウ集、活用モデル、取引モデルのイメージ

5. スケジュール、討議事項

今後の課題

前回TF資料

- SBOM実証および各企業へのヒアリング結果、タスクフォースにおける議論、国内外の動向等を踏まえ、今後の課題を下記のように設定。

令和3年度のSBOM実証および各企業へのヒアリング結果

- SBOM導入のための初期工数は発生するが、ツール活用により運用工数が低減。**管理対象のソフトウェアが多いほど効果が大きく**なり得る。
- ツールによる**脆弱性特定のリードタイムの短縮効果**を確認。
- 特に無償ツールは導入工数が大きく機能・精度も不十分。**ノウハウ共有**や**ツール自体の精度、機能向上**が必要。
- 開発者自身が**標準的なSBOMフォーマットで部品情報を共有**することが有効だが、**部品粒度等を揃える（要件化する）必要**。
- OSSの**再利用等も含め管理する場合のコスト**（精査工数等）が大きい。
- **管理対象のソフトウェアやステークホルダーが多い場合の実証**や、**繰り返し発生する脆弱性対応工数の評価**は未実施。

タスクフォースにおける議論（抜粋）

- **効果・コスト評価**（複数社の連携、システム規模の差、SBOMの更新）
- SBOM共有時の**コストや責任の分担**、**契約の整理**
- **自動化・ツール**（費用、精度、信頼性、相互運用性）
- メリットを享受できる**活用モデルの検討**
- **脆弱性の対応要否判断**
- **SBOMフォーマットや必要項目、管理単位、粒度の整理、標準化**
- **中小企業**への配慮、巻き込み
- **ノウハウの共有**（プラクティス集、ガイドライン）
- **政府機関での活用**（実証の実施、政府統一基準）

国内外の動向等

- 大統領令に基づき、米国政府調達におけるSBOM提供の**義務化に向けた動き**が進展。**SBOMの最小要素**公表。
- CISA SBOM a ramaでは、今後の主要な課題が抽出。（SBOM生成に必要な**データの提供方法**、SBOM共有・活用**ツール**、**各国の規制基準**への適用、SBOM**共有にあたっての信頼性や完全性**の確保 等）
- **医療機器分野では、IMDRFガイダンスに基づき、国内でも規制改正によるSBOM提供義務化**の動き。

今後の課題

1. SBOM活用モデルの最適化

- SBOMの作成主体や作成対象範囲、作成手段等によりコストや効果が異なり、産業分野によっては規制等の動きもあるため、**産業分野の状況に応じたSBOMの効果的な活用モデルを整理**。

2. SBOM共有のための環境整備

- **多数のステークホルダーがSBOMを共有・活用するケースの実証**。
- 各分野等における標準的な**SBOMの項目、粒度、フォーマット、部品命名規則等の整理**。
- **契約、責任、費用負担**の整理。

3. ツールの活用促進による効率化

- SBOMツールの導入や利用方法に係る**情報発信、ノウハウの共有による導入工数の低減**。
- ツール自体の**機能および精度向上**。

4. 国際的な基準との整合性確保

- グローバルサプライチェーンにおいて国内と海外の整合性を確保しつつ効率的に部品管理を行うためには、**国内外の基準の整合化**が必要。

今年度以降の取組

前回TF資料

- 前頁で設定した課題から、次年度以降の取組を下記のように整理。

令和4年度以降の取組	関連する前頁の課題	実施時期	実施主体
①実証によるコスト・効果の評価と論点整理の継続 規制等が進む分野やSBOM導入効果が大きい分野等を候補に、複数分野で実証を行うとともに、コスト・効果の評価、個別の課題等に係る知見を共有。成果を他の取組においても活用。	1、2	R4年度	国・民間
②SBOMの効果的な活用モデルの検討 各産業分野における規制の内容やリスク等を踏まえた、効率的／効果的な活用モデル（分野ごとの標準的なSBOM作成主体、対象部品、手段、データ形式・項目等）、およびステークホルダーの合意形成の在り方について検討。	1、2	R4年度	国
③SBOM共有に関する取引モデルの検討 サプライチェーンの部品管理に関する責任、部品情報共有の要件化、費用負担等、取引契約における論点を整理。産業分野ごとの取引契約書モデル等を検討。	2	R4年度以降	国・民間
④SBOMに関するノウハウ共有 実証で得たSBOMツールのノウハウ、コスト情報等についてガイド／手引きを作成。 NTIAのプレイブック等との対応も意識し、調整が必要な事項を整理。	3	R4年度	国
⑤SBOM自動化・共有に向けた技術的な検討 SBOMツールの調査、SBOMに係る基準や国際標準等への対応、構成管理ツールとの統合、脆弱性DBにおけるソフトウェアの識別子の整備、SBOM信頼性確保等に向けた検討や研究開発。	1、3、4	R4年度以降	国・民間 （国はツールの研究開発に関する技術課題の整理等を実施）
⑥国外との制度調和 米国と意見交換や成果の共有ができる関係を維持。制度等、必要な調整を実施。	4	R4年度	国

1. 昨年度のタスクフォースにおける議論の振り返り

2. ソフトウェアの管理手法等に関する国外の状況

3. 令和4年度のSBOM実証イメージ

4. ノウハウ集、活用モデル、取引モデルのイメージ

5. スケジュール、討議事項

【米国】ソフトウェアサプライチェーンのセキュリティ強化のためのガイダンス

- 2022年5月、NISTは、大統領令で指示された**ソフトウェアサプライチェーンのセキュリティ強化に向けたガイダンスを、SP 800-161**（Cybersecurity Supply Chain Risk Management (C-SCRM) Practices for Systems and Organizations）**のRev. 1の付録及び専用のWebサイトにおいて公開**した。
- NISTは、**関連する大統領令文書との相互な関わりを促進する**とともに、**SP 800-161に影響を与えることなく本ガイダンスの更新を可能とするためにWebサイトでの公開を行った**としている。
- 本ガイダンスでは、**大統領令に対するNISTの取組とSP 800-161 Rev.1で規定されたC-SCRMの管理策との対応関係**や、**ソフトウェアサプライチェーンのセキュリティ確保のための新たな概念**を概説している。
- NISTは連邦政府機関に対して、**本ガイダンスを活用してC-SCRMの管理策を調達先に対して適用すること**のほか、**可能な場合に新たな概念を採用すること**を求めている。

大統領令に対するNISTのこれまでの取組とC-SCRMとの対応関係

大統領令で指示されたソフトウェアサプライチェーンに関する3つの取組と、NIST SP 800-161 Rev.1やC-SCRMの管理策との対応関係について概説。

「重要なソフトウェア」の定義と求められる対策	• 各政府機関が優先的にセキュリティ対応を行う対象となる「重要なソフトウェア」の定義及び「重要なソフトウェア」のセキュリティ対策に関する取組。 • **C-SCRMの管理策や補足ガイダンスは、「重要なソフトウェア」に求められるセキュリティ対策を実施するための有効な手段**である。
開発者と消費者のためのソフトウェアサイバーセキュリティ	• ソフトウェア開発を安全に実施するため、開発者が準拠すべき対策（SSDF）と、消費者が開発者へ要求すべき最低限の推奨事項に関する取組。 • **C-SCRMの管理策や補足ガイダンスを用いて、開発者へ要求すべき最低限の推奨事項を確認**できる。
ソフトウェア検証の最低基準	• サプライヤー（ベンダーや開発者など）によるソフトウェア検証の際に推奨される最低基準に関する取組。 • **C-SCRMの管理策や補足ガイダンスを用いて、最低基準を満たしたソフトウェア検証が実施されていることを確認**できる。

ソフトウェアサプライチェーンのセキュリティ確保のための新たな概念

新たな4つの概念について、それぞれの事項を実施する際に各省庁が留意すべき点、各概念を採用することによる効果、今後の発展可能性を概説。

SBOM	• 各省庁は、ソフトウェア製品やサービスのサプライヤーが、**大統領令及びNTIAが公表しているガイドラインに準拠したSBOMを作成していることを確認すべきである**。
サプライヤーにおけるリスク評価の強化	• サプライヤーが作成したソフトウェアだけではなく、**サプライチェーンにおいてソフトウェアに関与する事業体に対してもリスク評価を強化すべき**である。
OSSの管理	• 各省庁は、**サプライヤーのソフトウェアにおけるOSSの使用状況をより深く理解するよう努めるべき**である。
脆弱性管理	• ゼロトラストアーキテクチャの議論を踏まえ、**各省庁の戦略は、検出された脆弱性をいかに効率的かつ包括的に管理するかについて焦点を当てるべき**である。

出所）NIST, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations Rev.1 https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final, Software Security in Supply Chains https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains

【米国】医療機器の市販前サイバーセキュリティガイダンスの改定案の公開

- 2022年4月、FDAは、**FDA申請※1の際に医療機器メーカーが含めるべきサイバーセキュリティ対策に関する推奨事項を示したガイダンス案**を公開し、パブリックコメントを開始した。（2022年7月7日まで。）
- ガイダンス案では、**医療機器に含まれる既製ソフトウェアコンポーネントに対して機械判読可能なSBOMを作成し、FDAに提出すること**、**既知の脆弱性を有するサードパーティのソフトウェアコンポーネントに対して、当該脆弱性に対するリスク評価結果とセキュリティ管理策をFDAに提出すること**を推奨しているほか、**医療機器の品質システム規制（QSR）においてSBOMを活用可能**であるとしている。
- なお、FDAのガイダンス文書は、発行時点でのFDAの考えや推奨事項を記述するものであるため、法的強制力はないが、規制当局から発表されるガイダンスであるため一定の影響力を有している。

※1 米国での医療機器販売のために必要な、FDAによる審査・承認のための申請のこと。

FDA申請を行う医療機器メーカーに対するソフトウェアコンポーネントに関連する推奨事項

既製ソフトウェアコンポーネント※2に関する機械判読可能なSBOMの生成・提出	• 医療機器に含まれる既製ソフトウェアコンポーネントについて、以下の要素をSBOMに含めること。 ✓ 当該ソフトウェアコンポーネントを含んでいる資産名称 ✓ 当該ソフトウェアコンポーネントの名称 ✓ 当該ソフトウェアコンポーネントのバージョン ✓ 当該ソフトウェアコンポーネントの開発者 ✓ 開発者により提供される保守・監視による当該ソフトウェアコンポーネントのサポートレベル ✓ 当該ソフトウェアコンポーネントのサポート終了日 ✓ 脆弱性データベースで公開されている当該ソフトウェアコンポーネントにおける既知の脆弱性 • SBOMは、機械判読可能な形式とし、業界標準のフォーマットを利用すること。 • FDAの審査・承認を支援するため、FDAに対してSBOMを提出すること。なお、上記の要素がSBOMに含まれていない場合、FDAによる審査を効率化するために、その旨を付加的にFDAに提供すること。
サードパーティのソフトウェアコンポーネントに関するリスク評価結果・セキュリティ管理策の提出	• 既知の脆弱性を有するサードパーティのソフトウェアコンポーネントについて、各脆弱性の安全性及びセキュリティに関するリスク評価を行い、その情報をFDAに提出すること。 • 各脆弱性に対処するために適用されるセキュリティ管理策を詳細化し、その情報をFDAに提出すること。

※2 医療機器メーカーが用いる一般に入手可能なソフトウェアコンポーネントのうち、当該メーカーによるソフトウェアライフサイクル全体を通じた管理が主張できないコンポーネントのこと。

出所）FDA, ”Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions Draft Guidance for Industry and Food and Drug Administration Staff”
https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions

（参考）【米国】医療機器の市販後サイバーセキュリティガイダンス

- 2016年12月、FDAは**医療機器メーカーの市販後のセキュリティ対策に関するガイダンス**を発行した。
- 医療機器メーカーにおいて**設計、開発、製造、流通、配備、保守を含む製品のライフサイクル全体**を通じたサイバーセキュリティに取り組むことが推奨されているほか、医療機器の市販後管理の一環として、**サイバーセキュリティ上の脆弱性や悪用可能性を監視、特定し、対処する必要性**を強調している。
- また、医療機器の安全又は基本性能を危うくする情報、患者に深刻な健康上の悪影響や死をもたらす情報については、**医療機器メーカーは、規制当局に通知**する必要がある。

市販後の医療機器に関するサイバーセキュリティガイダンスの概要

市販後における サイバーセキュリティリスク管理 プログラム	• サイバーセキュリティの脆弱性とリスクを特定・検知するためのサイバーセキュリティに関する情報源のモニタリング • 以下のメカニズムを含む堅牢なソフトウェアライフサイクルプロセスを維持 -サードパーティのソフトウェアコンポーネントの新たな脆弱性の監視 -OTSソフトウェア関連を含めた脆弱性を修正するためのソフトウェアアップデート及びパッチの検証と妥当性確認 • 脆弱性および存在と影響の理解、評価、検知 • 脆弱性の取り込みと対処に関するプロセスの確立と伝達 • 脅威モデリングを用いたサイバーセキュリティリスクから保護、対応、復旧するための緩和策を開発。機器の安全性と本質的な性能を維持する方法に関する明確な定義 • 協調的な脆弱性開示の方針と実践 • サイバーセキュリティリスクに早期かつ悪用される前に対処する軽減策の配備
情報共有	• 医療機器および医療ITコミュニティ間の連携を促進し、医療機器のサイバーセキュリティの脆弱性がもたらすリスクについて共通の理解を得ることを目的としている。 • 医療機器の安全又は基本性能を危うくするもの、患者に深刻な健康上の悪影響や死をもたらすものについては、医療機器メーカーは規制当局まで通知する必要がある。 • ISAO （Information Sharing and Analysis Organizations：情報共有分析機関）の１つであるNH-ISACに加盟することを推奨している。

出所）FDA, ”Postmarket Management of Cybersecurity in Medical Devices Guidance for Industry and Food and Drug Administration Staff”
https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices

（参考）【米国】VEXドキュメントに含めるべき最小要素の公開

- 2022年4月、CISAは、**Vulnerability Exploitability eXchange（VEX）ドキュメントに含めるべき最小要素を示した文書**を公開した。
- **VEXドキュメントとは、ある製品が既知の脆弱性の影響を受けるかどうかを示す機械判読可能なセキュリティ勧告の一形態**であり、CISAは、**VEXドキュメントの最小要素として、メタデータ、製品の詳細、脆弱性の詳細、脆弱性のステータスを含めるべき**としている。
- CISAは、今後、VEXの仕様改良、VEXの活用促進に向けた実用的なガイダンスの提供などを検討するとしており、将来的には、**脆弱性管理に係るエコシステムの自動化においてVEXを活用することを目標**としている。
- なお、VEXは、**SBOMを活用した脆弱性管理を更に効率化するために開発**されたが、**必ずしもSBOMにVEXを含める必要性はなく**、また、**VEXを活用する際にもSBOMと併用する必要はない**としている。

最小要素の項目	最小要素の具体的な定義
VEXドキュメントのメタデータ	VEXドキュメントのメタデータについて、以下の情報を含めること。 • VEXフォーマットの識別子 • VEX文書の作成者 • VEX文書のタイムスタンプ • VEX文書の識別文字列 • VEX文書の作成者の役割
製品の詳細	VEXドキュメントの対象製品について、以下のいずれかの情報を含めること。 • 製品の識別子 • 製品群の識別子（例：一意の識別子、サプライヤー名・製品名・バージョン文字列の組み合わせ）
脆弱性の詳細	対象製品に存在する脆弱性について、以下の情報を含めること。 • 脆弱性の識別子（CVEまたは他の識別子） • 脆弱性の説明（例：CVEの説明）
脆弱性のステータス	対象製品に存在する脆弱性のステータスについて、以下のいずれかの情報を含めること。 • 影響を受けない（NOT AFFECTED）：脆弱性について、対策は必要ない状態 • 影響を受ける（AFFECTED）：脆弱性を対策または対処が推奨される状態で、脆弱性に対する対処策も情報として含める • 修正済み（FIXED）：脆弱性に対する修正がされている状態 • 調査中（UNDER INVESTIGATION）：脆弱性の影響を受けるかどうか不明な状態

出所）CISA, ” Vulnerability Exploitability eXchange(VEX) – Use Cases”
https://www.cisa.gov/sites/default/files/publications/VEX_Use_Cases_Document_508c.pdf

（参考）オープンソース・ソフトウェア・サミット

- 2022年1月、**米国家安全保障会議（NSC）によりオープンソース・ソフトウェア・サミットが開催**され、政府・産業界から参加（Linux FoundationとOpenSSFが実施面をフォロー）。
- 2022年5月に第2回が開催され、Linux FoundationとOpenSSFから**オープンソースとソフトウェアサプライチェーンセキュリティに対応するための実行計画（３つの目的と10項目）が公表**されたところ、日本においても8月下旬に本取組に関する会合が予定されている。

＜実行計画の３つの目的と１０項目＞

	目的	項目	概要
1	①オープンソースセキュリティ製品の保護	セキュリティ教育	ベースライン・セキュア・ソフトウェア開発の教育と認定を全ての人に提供
2		リスクアセスメント	上位10,000以上のOSSコンポーネントをベンダー中立かつ客観的なリスク評価のためのダッシュボードを確立
3		デジタル署名	ソフトウェアリリースにおけるデジタル署名の採用を加速
4		メモリ安全性	メモリ非安全なプログラム言語をメモリ安全な言語に置き換えることで多くの脆弱性の根本原因を排除
5	②脆弱性検出と修正の強化	インシデント対応	OpenSSFのオープンソース・セキュリティ・インシデント対応チームを確立し、セキュリティ専門家が脆弱性対応の重要局面を支援
6		スキャニング改善	高度なセキュリティツールと専門家のガイダンスを通じた新たな脆弱性の発見を加速
7		コード監査	年に1回、最大200個の最も重要なOSSコンポーネントのサードパーティによるコードレビュー（及び必要な修復作業）を実施
8		データ共有	業界全体のデータ共有を調整し、最も重要なオープソース・ソフトウェアを特定するための調査を改良
9	③パッチ対応時間の短縮	SBOMの普及	SBOMツーリングとトレーニングを改良し、SBOMの導入を促進
10		サプライチェーンの改善	より優れたツールとベストプラクティスにより最も重要な10個のオープンソース・セキュリティのビルドシステム、パッケージ・マネージャ、ディストリビューション・システムを強化

出所）https://www.linuxfoundation.org/press-release/linux-foundation-openssf-gather-industry-government-leaders-open-source-software-security-summit/

1. 昨年度のタスクフォースにおける議論の振り返り

2. ソフトウェアの管理手法等に関する国外の状況

3. 令和4年度のSBOM実証イメージ

4. ノウハウ集、活用モデル、取引モデルのイメージ

5. スケジュール、討議事項

本年度SBOM実証の進め方

実証の目的・基本方針に基づき、産業分野ごとの法制度等を考慮して、期待されるSBOM活用モデル(案)を検討し、その実現に向けて検証すべき仮説、比較評価項目を設定し、実証を通じて活用モデルの妥当性を確認する。

実証実施手順

凡例： 経産省、MRIが共同で実施 / 実証事業者中心に実施 / 経産省、MRI、実証事業者が共同で実施

(1)目的・基本方針の設定 → (2)実証対象分野・事業者の候補選定 → (3)分野ごとの前提条件等の整理 → (4)実証の設計 → (5)実証実施・進捗管理 → (6)実証結果の評価分析

(3)分野ごとの前提条件等の整理

- **対象分野における前提条件の整理**
  - SBOMに係る法制度上の基準、推奨事項（SBOMに関する要求事項）
  - 業界における部品管理の現状
  - 業界のサプライチェーン構造や取引慣行
  - 管理対象のソフトウェアの特徴（組込系／情報系、言語、規模など）
- **重視すべき観点の整理**
  - SBOM作成、活用におけるコスト、技術等の課題

(4)実証の設計

- **SBOM活用モデル検討の枠組み整理**
  - SBOM適用項目の選択肢の整理
    SBOMの適用項目に関してコスト・効果への大きさをもとに主要な選択肢を俯瞰的に整理する。
  - 分野ごとのSBOM活用モデル案の検討
    分野において期待されるSBOM適用範囲のモデルケース案について、選択肢の組合せにより検討。
- **実証項目の整理**
  - SBOM活用モデル案の妥当性を確認するため、選択肢の比較評価項目の設定および検証すべき仮説の整理

(6)実証結果の評価分析

- **実証結果の評価**
  - 比較評価項目に関するコスト、効果等の計測・評価、仮説の検証結果をもとに、各分野における効果的なSBOM活用モデルを改訂。
- **想定する成果物**
  - 分野ごとに期待されるSBOM活用モデル（適用範囲）を整理したガイダンス
  - サプライチェーン取引におけるSBOMの導入促進のための取引契約モデルのガイダンスに係る論点整理
  - 各分野におけるSBOM適用ノウハウ、プラクティス、実証による知見をまとめたガイダンス

SBOM活用モデルの検討イメージ

前回TF資料

- SBOMの作成・活用においてコストや効果に対する影響の大きい選択肢を整理し、実証の対象分野における妥当な組合せを検討。実証による評価を通じて活用モデルを整理。

STEP1　SBOM活用モデルの検討における選択肢の整理

＜整理例＞

区分	選択肢（コスト・効果への影響が大きいものを想定）
(a) 作成主体	(a1)ベンダーのみ
	(a2)ベンダー＋サプライヤー（受託開発）
	(a3)ベンダー＋サプライヤー（受託開発）＋サプライヤー（既成部品ベンダー、サードパーティ・OSSベンダーを含む。）
(b) 対象部品	(b1)直接利用する部品のみ（ビルドツール、構成ファイルなどを利用できる）
	(b2)間接的・再帰的に利用する部品まで（商用ツール利用が前提か）
(c) 作成手段	(c1)手動で特定・作成
	(c2)ツールで作成・精査無し
	(c3)ツールで作成・手動で精査
(d) データ形式・項目	(d1)標準フォーマット（SPDX、SPDXLite等）
	(d2)大統領令最小要素を含む
	(d3)上記を満たさない
(e) 活用の範囲	(e1)脆弱性の特定
	(e2)脆弱性の深刻度評価
	(e3)ライセンスの特定

STEP2　各分野における妥当な組合せを検討

＜考慮事項の例＞

- 規制等における要求事項
- サプライチェーン構造や商慣習
- リスクの大きさ　　等

STEP3　実証による評価

- 実証におけるSBOM活用のシナリオを設定。
- 各分野、各シナリオにおけるコスト、効果を評価。
- **評価結果を踏まえ、各分野における効果的、効率的なSBOM活用モデルを整理**。

本年度SBOM実証の対象分野

- **SBOMに関して「規制や推奨化が見込まれる分野」や「効果が大きいと思われる分野」を候補**に、本年度の実証では、**医療機器分野、自動車分野、ソフトウェア分野でのSBOM実証を実施**する。
- **分野ごとの法制度における要求、コスト・効果の受容性などに基づき、分野ごとに期待されるSBOM活用モデルを検討する。**実証等で得られた知見を分野間で共有し、SBOM導入促進のためのガイダンスに反映する。
- 実証分野以外については、実証結果をもとに最小限求められるSBOM活用モデルを検討する。

① 医療機器分野
（医療機器メーカー等）

② 自動車分野
（OEM/部品サプライヤー等）

SBOMに関する規制や推奨化が見込まれる分野

知見を共有

③ ソフトウェア分野
（ITベンダーとそのサプライチェーン等）

SBOMの効果が大きいと思われる分野

- 規制等において定められる**SBOMへの要求事項を満たしつつ、SBOMを効率的に作成、活用していくモデル**（作成者、作成／共有方法、最低限含むべき項目やフォーマット等）を検討。
- 米国NTIAにおける既存のPoCについて得られる情報を確認、活用。

- 社内システムおよび顧客向け**システム／サービスを多く管理**し、**SBOMを多様なサプライヤーやユーザーと共有**するうえで、**メリットを最大限享受できる活用モデル**の検討。
- 開発環境や構成管理ツール等との連携など、ツール環境に関する知見や課題の整理。

分野ごとの前提条件等の整理

- 産業分野によっては規制等の動きもあるため、**産業分野の前提条件等についてまとめ、実証で重視すべき観点について整理**。

前提等		医療機器分野	自動車分野	ソフトウェア分野
①分野の前提・傾向、業界のサプライチェーン構造や商慣習の特徴など		• ソフトウェアの委託開発階層は一段階程度。 • 医療機器の特性より精度の高いSBOMが求められる。一方で、中小開発企業やサプライヤーについては、SBOMの導入ができていない。	• サプライチェーンは階層構造になっており、中小、海外も含めて複雑に絡み合っている。 • 全サプライヤーが有償SBOMツールを用いることのコスト負担が大きい。	• SBOM生成の主体となるケースが多い。 • SBOM生成・管理そのものがビジネスにつながる可能性がある。
②規制対象及び規制内容		• 米国IMDRFガイダンスや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（パブコメ中）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。	• 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や各車両に使用されるソフトウェアに関するSBOMの作成・維持が求められる可能性あり。 • 各国法規で参照される国連規則UN-R155の要求事項において、ソフトウェア構成管理や部品表の作成を例示している。	• 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)。
③管理対象のソフトウェアの特徴（組込／Web、言語、規模など）		• 既製ソフトウェア（商用、のことで（Windows製品等）は利用もOSSは避ける傾向あり • 購買、開発委託が主流（多種多様な医療機器があるため、規模感は多様）。	• ハードウェア製品内に組み込まれたソフトウェア（ファームウェア）も多い。 • 制御系/情報系に分けられ、前者はC言語が多く、後者ではOSSの導入が増えている。（仮説） • バイナリでの納品も多い。（仮説）	• Java，C/C++，Python、JavaScriptなど多様な言語が用いられる。 • クラウド、SaaSなどWebベースのアプリケーションも含まれる。
上記①から③までを踏まえ、各分野の実証で重視すべき観点	**SBOMの作成・提供**	• 精度の高いSBOMを作成し、提供する必要がある一方で、中小企業にも配慮した作成方法（主にツール利用コスト）を検討する必要あり。	• 多数のサプライヤーからのSBOMを共通形式で取得し、自動処理することが期待される。 • 間接利用部品は、ティア１が一括でSBOM生成することの実現性を確認することが必要。	• 相互運用可能なフォーマットで作成する必要がある。 • 最終製品ベンダーにおいて、間接利用部品のSBOMの精査をすることの実現性を確認することが必要。
	SBOMの運用・管理	• 医療機器を利用する医療機関においてもSBOM利活用が求められる。	• サプライチェーンを通じた脆弱性情報の共有が求められる。	• 相互運用可能なフォーマットで作成・共有・運用する方法を定義することが求められる。

※１：直接利用部品：　サプライチェーンにおいて契約関係のある開発者が直接利用する部品
※２：間接利用部品：　サプライチェーンにおいて契約関係のないサプライヤ（サードパーティ）が提供する部品から再帰的に利用される部品

分野別SBOM実証の範囲について

- SBOMのあらゆるユースケースを一つの実証でカバーするのは困難。
- 分野ごとの前提等にあわせた実証を行うことで、その有効性や課題の整理を行っていく。

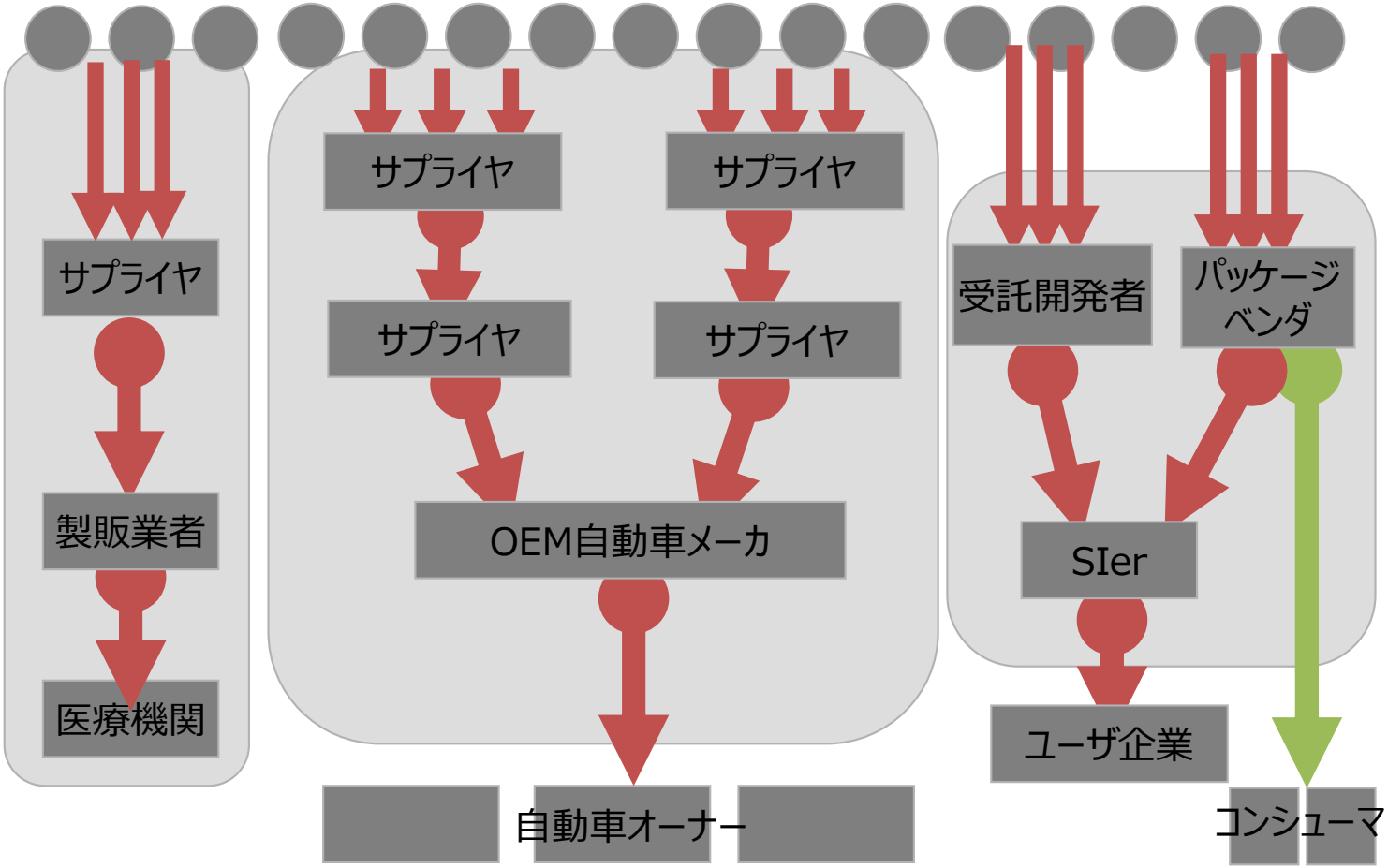
ソフトウェア（OSS含む）

サプライヤ
（システム、ソフトウェア）

製販業者・インテグレータ

ユーザ事業者

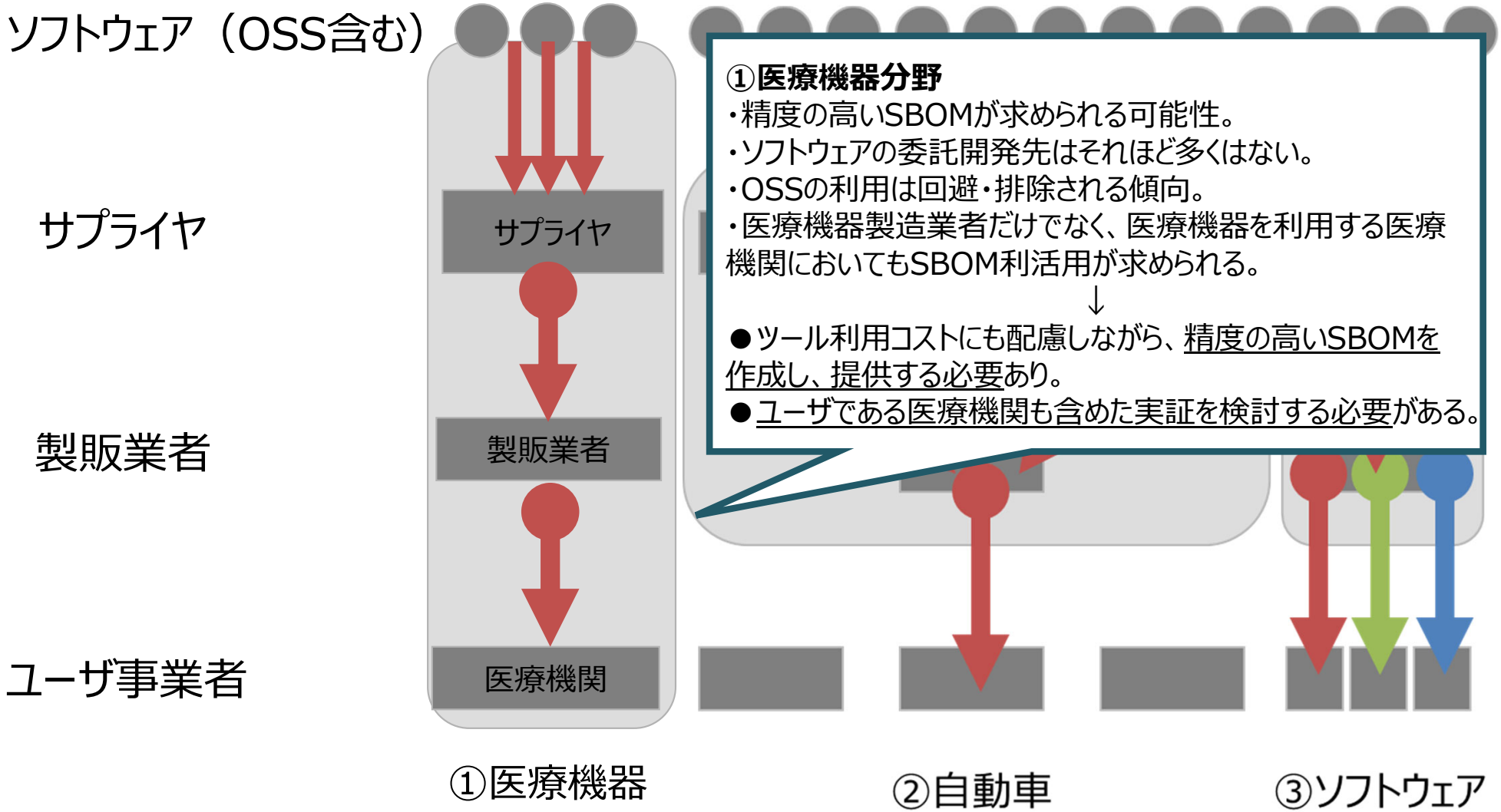
コンシューマ



①医療機器　②自動車　③ソフトウェア

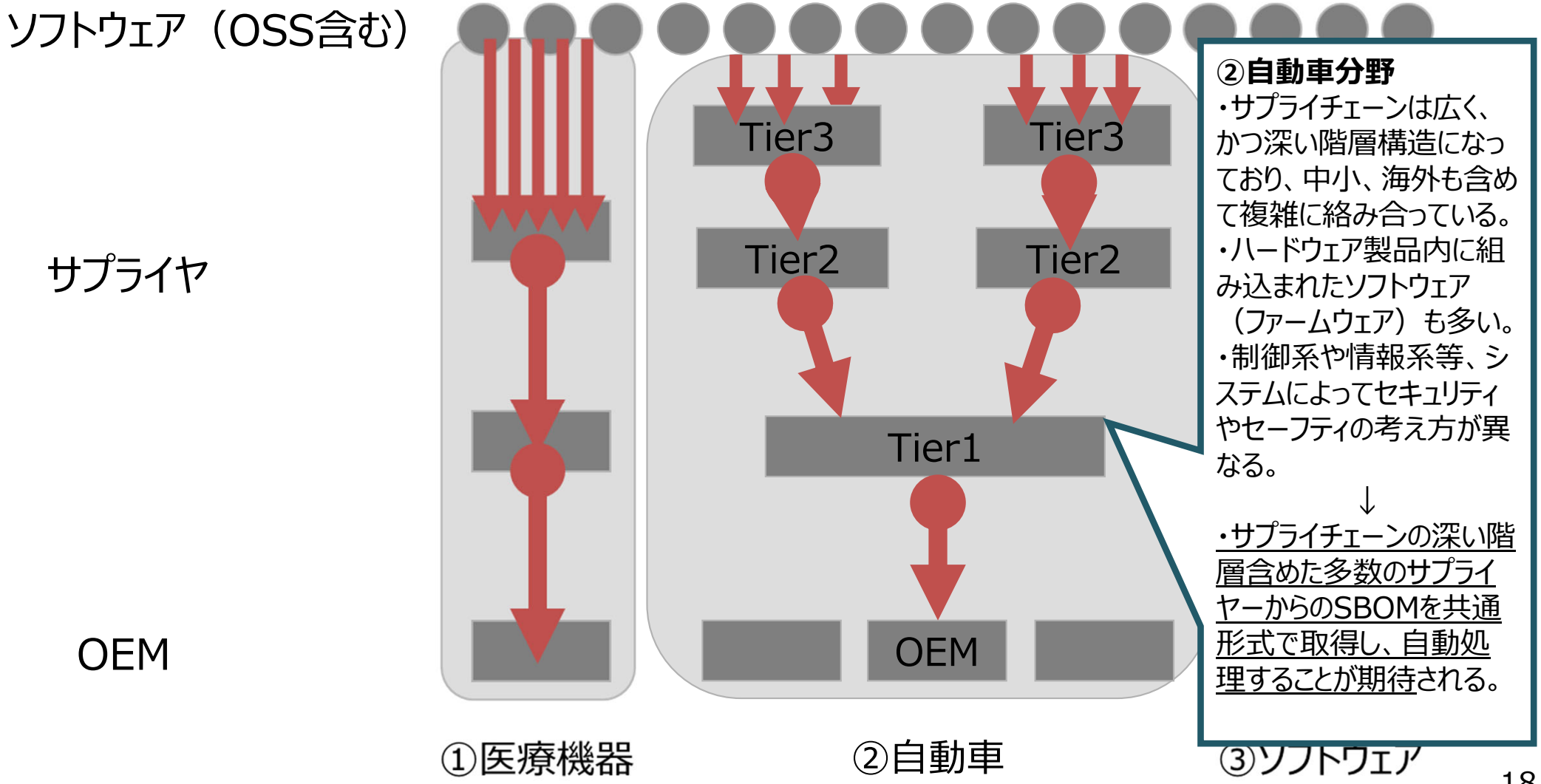
分野別SBOM実証｜①医療機器分野

- 法制度の要求に合わせた精度の高いSBOMの生成・管理が求められる。
- 医療機関（ユーザ事業者）によるSBOM活用の可能性を検討。



分野別SBOM実証｜②自動車分野

- 契約関係にあるサプライヤのSBOM生成による信頼性の確保とサプライチェーンを通じたコスト低減
- ティア１等によりサプライチェーンの契約関係外のサプライヤ（既製品）等のツールを用いたSBOMの一括生成による効率化。



②自動車分野

・サプライチェーンは広く、かつ深い階層構造になっており、中小、海外も含めて複雑に絡み合っている。

・ハードウェア製品内に組み込まれたソフトウェア（ファームウェア）も多い。

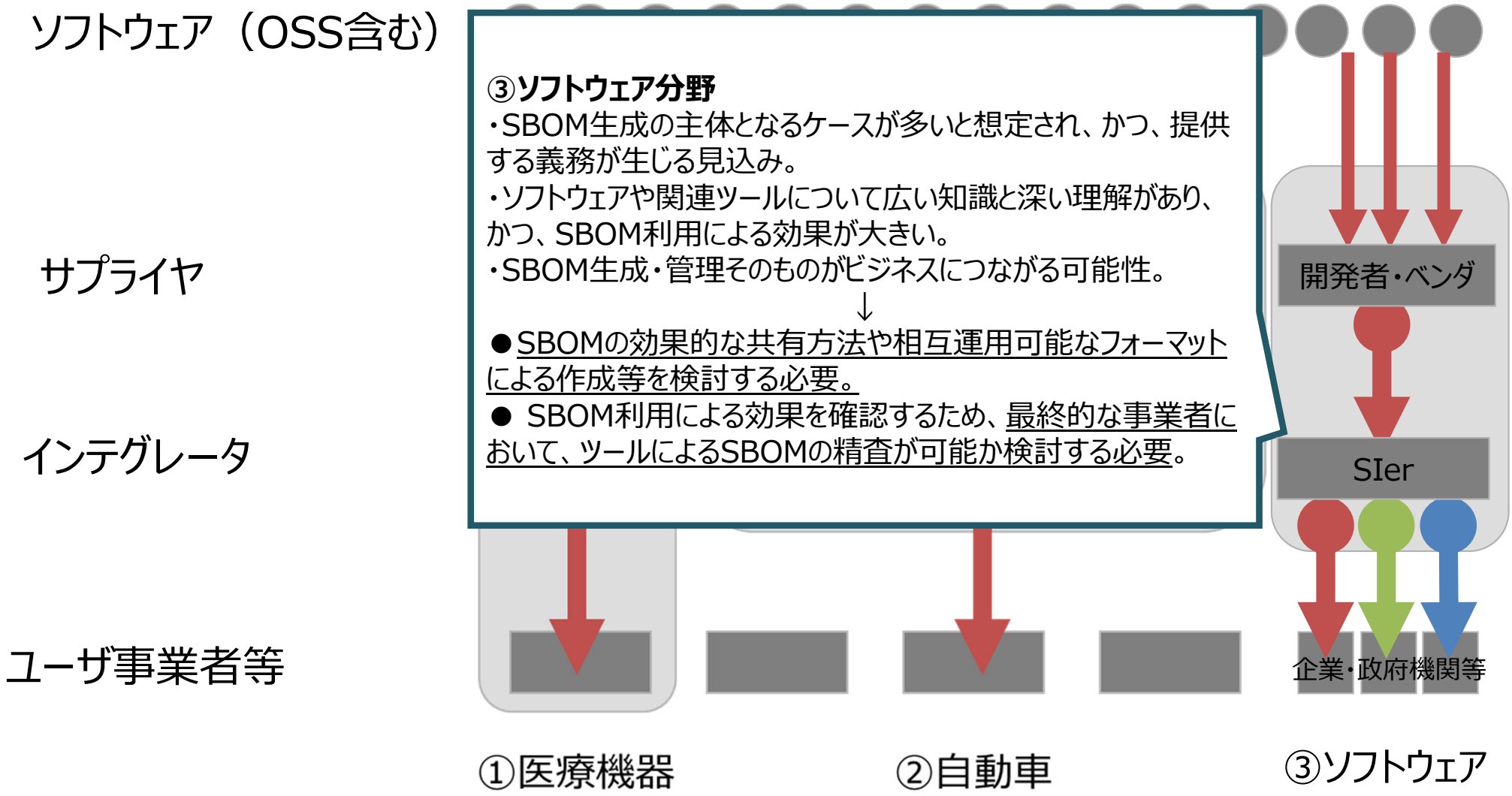
・制御系や情報系等、システムによってセキュリティやセーフティの考え方が異なる。

↓

・サプライチェーンの深い階層含めた多数のサプライヤーからのSBOMを共通形式で取得し、自動処理することが期待される。

分野別SBOM実証｜③ソフトウェア分野

- 機器ベンダ、SIerによるサプライチェーンを通じたSBOM一括生成による効率化。
- OSSの知見を活用したSBOM精査による信頼性の確保



SBOM適用項目の選択肢の検討方法

- SBOMの適用に関する選択肢は、昨年度からの調査・実証に基づき、下記のとおり、案として整理。産業分野横断的に俯瞰して、コスト・効果の観点で大きく影響する項目を特定し、**分野ごとに適用範囲の共通的な認識ができるように整理**する。

SBOM適用に関する主な選択肢の整理案

	適用区分	主な適用項目（選択肢）	コスト感
SBOM生成・共有	(a)SBOM作成主体 (Who)	(a1)自社	小
		(a2)サプライヤ（開発委託先）取引契約あり	中
		(a3)サプライヤ（サードパーティ）取引契約なし	大
	(b)作成範囲 (What, Where)	(b1)直接利用部品（開発主体が直接利用する部品）	小
		(b2)間接利用部品（既製品など開発委託契約のない部品から再帰的に利用する部品）	大
	(c)作成・検査手段 (How)	(c1)手動で特定（構成管理情報利用）・ツールで生成	小
		(c2)ツールで特定・生成・誤検知精査なし	小
		(c3)ツールで特定・生成・誤検知精査あり	中
		(c4)開発委託元が、開発委託先の作成したSBOMを独立に検査	大
	(d)データ様式・項目 (What)	(d1)標準フォーマット（SPDX、CycloneDX、SPDX Lite等）	中
		(d2)大統領令におけるデータフィールドの最小要素を含む	小
		(d3)上記を満たさない要素	小
SBOM活用	(e)活用の範囲 (Why)	(e1)脆弱性の特定	小
		(e2)脆弱性の深刻度評価	小
		(e3)脆弱性の悪用可能性等の評価と対処	中
		(e4)ライセンス特定	中
	(f)活用主体 (Who)	(f1)製品利用者	小
		(f2)最終製品ベンダー	中
		(f3)各部品の開発者	大

（参考）SBOMの最小要素等と各フォーマットの項目との対応関係について

最小要素等	SPDX	SPDX Lite	CycloneDX	SWID
①サプライヤー名 (Supplier Name)	PackageSupplier		Supplier publisher	<Entity>@role(softwareCreator/publisher),@name
②コンポーネント名 (Component Name)	PackageName	PackageName	name	<softwareIdentity>@name
③コンポーネントのバージョン(Version String)	PackageVersion	PackageVersion	version	<softwareIdentity>@version
④その他の一意な識別子(Unique Identifier)	DocumentNamespace combined with SPDXID	Package SPDX Identifier	bom/serialNumber component/bom-ref	<softwareIdentity>@tagID
⑤依存関係 (Relationship)	Relationship:CONTAINS		(Inherent in nested assembly/subassembly and/or dependency graphs	<Link>@rel, @href
⑥SBOMの作成者 (Author Name)	Creator	Creator	metadata/authors/author	@role(tagCreator), @name
⑦タイムスタンプ (Timestamp)	Created	Created	metadata/timestamp	<Meta>
⑧コンポーネントハッシュ(Component Hash)	PackageChecksum Or VerificationCode		Hash “alg”	<Payload>/../<File>@[hash-algorithm]:hash

出所）[1] NTIA, “Survey of Existing SBOM Formats and Standards”, 2021
[2] SPDX® Specification Version 2.2.2, & G.3 Table of SPDX Lite fields

1. 昨年度のタスクフォースにおける議論の振り返り

2. ソフトウェアの管理手法等に関する国外の状況

3. 令和4年度のSBOM実証イメージ

4. ノウハウ集、活用モデル、取引モデルのイメージ

5. スケジュール、討議事項

ノウハウ集・活用モデル・取引モデルについて

- 導入ノウハウ集、活用モデル・ガイダンス、取引モデル・ガイダンスについて、昨年度の実証結果やタスクフォースでの議論等を踏まえ、目的を下記のとおり整理した。
- **これらの目的を踏まえ、次ページ以降のとおり、構成案を検討**。

文書	昨年度の実証結果・議論	文書作成の目的
①導入ノウハウ集	• 特に無償ツールは**導入工数が大きく**、機能・精度も不十分であり、**ノウハウ共有**（プラクティス集、ガイドライン）や**ツール自体の精度、機能向上**が必要である。	• SBOM作成者（ソフトウェア開発組織）が、**SBOMツールの導入や利用方法等について、理解を深める**ための導入ノウハウ集を策定し、導入工数の低減を図る。 • **SBOMの概要やSBOM導入に係る留意点を整理**することで、SBOMに関する適切な情報発信を図る。
②活用モデル・ガイダンス	• 開発者自身が**標準的なSBOMフォーマットで部品情報を共有**することが有効だが、**部品粒度等を揃える（要件化する）必要**がある。 • **SBOMフォーマットや必要項目、管理単位、粒度の整理、標準化を検討する必要**がある。 • **中小企業への配慮、巻き込みも考慮する必要**がある。	• 各産業分野における規制の内容やリスク等を踏まえた**効率的／効果的な活用モデル（分野ごとの標準的なSBOM作成主体、対象部品、手段、データ形式・項目等）やステークホルダーの合意形成の在り方を整理**し、各分野ごとの標準的なSBOMの活用モデルを示して、SBOMの効果的な活用を図る。
③取引モデル・ガイダンス	• SBOM共有時の**コストや責任の分担**、**契約のあり方について整理する必要**がある。	• **サプライチェーンの部品管理に関する責任、部品情報共有の要件化、費用負担等、取引契約における論点を整理**して、産業分野ごとの取引契約書モデル等を示し、SBOM活用のための環境整備を図る。

①SBOM導入ノウハウ集 目次構成案

- **ソフトウェア開発組織を主な対象者**とし、**SBOM導入を促進する**ためのノウハウ集を作成。
- ノウハウ集では、**SBOMの概要、定義、導入のメリット等のSBOMに関する基本的な情報**に加えて、**ツールの導入や利用方法等などのSBOM導入に向けたプロセス、各プロセスにおける具体的な導入ノウハウ、各プロセスにおける留意点等**を記載。

章	項	主な記載内容	実証項目との関係
1. 背景と目的	1.1 背景 1.2 目的 1.3 ノウハウ集の対象読者 1.4 ノウハウ集の対象ソフトウェア 1.5 ノウハウ集の活用方法	• ノウハウ集策定にあたっての背景や目的 • ノウハウ集が対象とする読者 • ノウハウ集が対象とするソフトウェア（単一ソフトウェア、アプリケーション、コンテナ、組込みソフトウェア 等）	３分野で実証を通じて、対象読者、対象ソフトを示す（初級者向けを想定。）。また、実証から特定される課題と解決ノウハウをもとに整理する。
2. SBOMとは	2.1 SBOMとは 2.2 SBOMの例 2.3 SBOM導入のメリット 2.4 SBOMに関する誤解	• SBOMの概要・定義 • SBOMの例（実証で得られたSBOMをベースとする） • SBOM導入による脆弱性管理上・ライセンス管理上のメリット • SBOMに関する誤解と事実	実証のコスト効果の評価結果に基づき、導入メリットのポイントを整理。 「SBOMとは」等の項目は、NTIA文書等の調査に基づく。
3. SBOM導入における基本指針	3.1 SBOM導入における基本指針 3.2 SBOM導入に向けた全体像	• SBOMに含めるべき要素（大統領令の最小要素など） • 採用すべきSBOMの形式（自動化サポートが可能な形式） • SBOM導入に向けたプロセスの全体像	各分野の実証から分野横断で共通する全体プロセスをまとめる。
4. SBOM導入ノウハウ	4.1 SBOM導入に向けた環境構築・体制整備におけるノウハウ 4.2 SBOMの作成におけるノウハウ 4.3 SBOMの共有におけるノウハウ 4.4 SBOMの活用におけるノウハウ	• SBOM導入に向けた環境構築手順、有用なツール等 • SBOM作成に向けて収集すべき情報 • SBOM導入に向け整備すべき体制 • SBOMの作成手順、ユーザーに対する共有手順 • SBOMの活用方法	実証におけるSBOM導入、生成・共有、活用の各フェーズからコストの低減や課題の解消法に係るノウハウを整理する。 ツール選択の考え方も含む。
5. SBOMに関する留意点	5.1 環境構築・体制整備における留意点 5.2 SBOMの作成における留意点 5.3 SBOMの共有における留意点 5.4 SBOMの活用における留意点 5.5 部品管理におけるリスクと課題 5.6 SBOMの知的財産権と機密保持	• SBOM導入プロセスにおける留意点（実証で明らかになった留意事項等） • 部品管理上のリスク及び課題 • SBOMの知的財産権や秘密保持において留意すべき事項	ノウハウ以外の留意点、リスクへの影響などについて整理する。
6. 付録	6.1 用語集 6.2 参考情報	• 用語集及び参考情報源	NTIA SBOM at a glanceの日本語訳等と整合させる。

②SBOM活用モデル・ガイダンスの構成案(分野ごとのSBOM適用範囲のモデルケース案)

- SBOM活用モデル・ガイダンスの全体構成は以下のような案を想定し、**今年度はこれらの主要な要素（分野ごとの標準的なSBOM作成主体、対象部品、手段、データ形式・項目等やステークホルダーの合意形成の在り方）について整理**。
- SBOM適用項目のコスト・効果については多数の組合せがあり、今年度実証で、比較評価できない項目組合せについては、例示という位置付け。

章	項	主な記載内容	実証項目との関係
1. 背景と目的	1.1 背景と問題認識 1.2 SBOM活用モデルの必要性 1.3 本書の目的	• SBOM普及における課題や問題認識等の背景を記載 • 問題認識に基づきSBOM活用モデルの必要性を示す。 • それらを踏まえて本書の目的を示す。	（昨年度調査・実証結果等に基づき整理。）
2. 概要	2.1 SBOM活用モデルとは？ 2.2 想定読者 2.3 本書の全体構成	• SBOM活用モデルの概要、対象読者についてまとめる。 • 本書の全体構成を示す。	３分野での実証に基づき対象者を示す（開発部署関係者を想定）。
3. SBOM活用モデルの考え方	3.1 基本的な考え方 3.2 活用方法	• SBOM活用モデルの基本的な考え方、活用方法についてまとめる。	実証結果全体をもとに考え方を整理。
3. SBOM活用モデルの枠組み	3.1 SBOMの適用区分と選択肢 3.2 SBOMの活用モデルの定義方法	• SBOM活用モデルの枠組みを定義する上で必要になる、適用項目の選択肢とそれらの組合せによる適用範囲について記載	SBOM適用選択肢の整理結果をもとに作成。
4.SBOMに関する法制度、条件等	4.1 法制度の全体概要 4.2 医療機器分野 4.3 自動車分野 4.4 ソフトウェア分野 4.5 その他分野	• SBOM活用モデルのコンセンサスを整理するにあたり前提となる法制度や条件などを分野ごとに整理する。	SBOM実証の前提条件等の調査検討結果に基づき整理。
5.産業分野ごとのSBOM活用モデル	5.1 検討アプローチ 5.2～5.4 各分野（医療機器分野、自動車分野、ソフトウェア分野） - 基本要件と考え方 - 活用モデル案 - 留意点とカスタマイズ	• SBOM活用モデルの検討アプローチを明示 • 分野ごとに、基本要件を踏まえた考え方の整理 • 分野ごとに、事業者、業界団体の意見をもとに検討整理した活用モデル案（適用範囲のモデルケース）の提示 • 活用モデルに関する留意点、カスタマイズ方法	分野ごとに実証するSBOM適用モデルケースに対するコスト評価、フィージビリティ検討結果に基づき整理。ただし、比較検証は部分的となる。
6. 付録	6.1 用語集と参考情報	• 参考となる情報源	関連文書に整合させる。

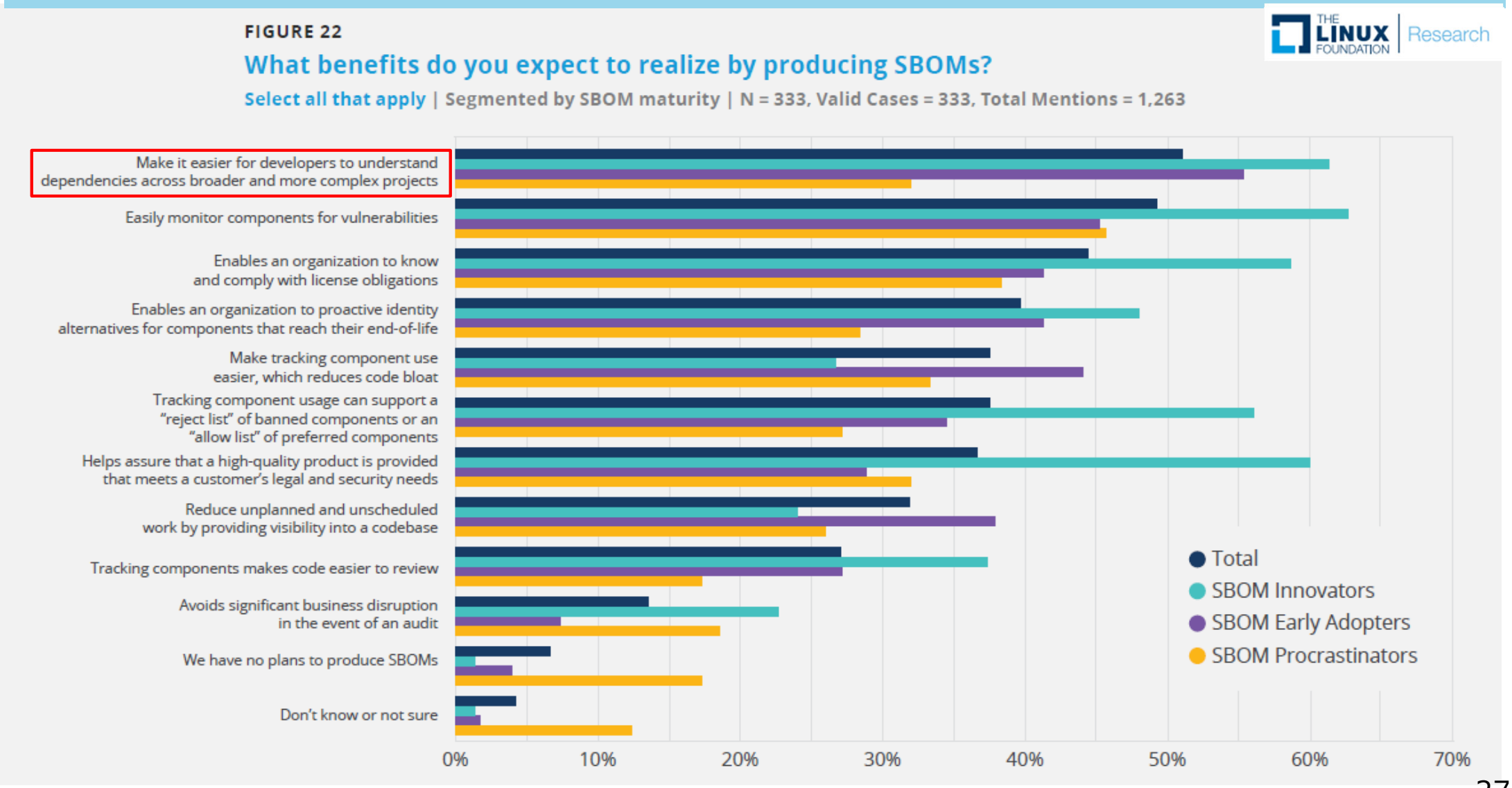
③SBOM取引モデル・ガイダンスの構成案（SBOM普及促進させるため取引契約モデルケース案）

- SBOM取引モデル・ガイダンスの全体構成は以下のような案を想定し、**今年度はサプライチェーンの部品管理に関する責任、部品情報共有の要件化、費用負担等、取引契約における論点などに関する検討・構成案の一部要素を整理**。

章	項	主な記載内容	実証項目との関係
1. 背景と目的	1.1 問題認識 1.2 SBOM取引モデルの必要性 1.3 本書の目的	• SBOM普及における課題や問題認識等の背景を記載 • 問題認識に基づきSBOM取引モデルの必要性を示す。 • それらを踏まえて本書の目的を示す。	（昨年度調査・実証結果等に基づき整理。）
2. 全体概要	2.1 SBOM取引モデルとは 2.2 対象読者 2.3 本書の全体構成	• SBOM取引モデルの概要、対象読者についてまとめる。 • 対象読者については、製品メーカー、サプライヤー、ユーザ企業などの候補について本書との関係性を示す。 • 本書の全体構成を示す。（主な内容は3～6章）	３分野での実証に基づき対象者を示す（契約担当部署、開発部署関係者を想定）。
3. 取引モデルの活用方法	3.1 SBOM取引モデルの考え方 3.2 SBOM取引モデルの活用方法	• SBOM取引モデルの基本的な考え方、活用方法についてまとめる。	実証結果全体をもとに考え方を整理。
4.責任関係の明確化	4.1 部品管理における役割と責任関係 4.2 ライセンス規約と脆弱性対応 4.3 損害賠償責任	• SBOMに係る規定の前提となる部品管理に関する役割や責任関係、ライセンス規約、脆弱性対応に関する規定例を示す。 • 損害賠償責任に関する規定例を示す。	文献調査、ヒアリングにより整理。（今年度は一部のみ調査）
5.SBOM管理	5.1 SBOM適用範囲に関する規定 5.2 SBOMの必要要素、フォーマットに関する規定 5.3 SBOMの信頼性に関する規定 5.4 SBOMの更新に関する規定 5.5 見積要求と費用負担	• 取引企業間のSBOMに関する具体的な規定例について示す。 • また、SBOMがサプライチェーンを通じて無理なく普及するように見積もりや費用負担に関する規定例を示す。	実証に基づき作成したSBOM活用モデル・ガイダンスをもとに、その後、契約条項の文献調査を踏まえてサンプルを整理。
6. プロセス・手順	6.1 プロセスの全体像 6.2 開発プロセスにおける手順等 6.3 運用プロセスにおける手順等	• SBOMに具体的に対応するためのプロセス・手順に関する規定を示す。	SBOM実証結果に基づき、その後、SBOM生成・活用の全体プロセスを整理。
7. 付録	7.1 用語集 7.2 参考情報・事例	• 用語集及び参考情報源	関連文書に整合させる。

（参考）SBOM生成により期待されるメリット

- 2021年にLinux Foundation Researchが実施した調査（412組織サーベイ調査）においては、**SBOMに係るメリットとして**、脆弱性への監視やライセンス義務への対応のほか、SBOMによりコンポーネントの依存関係が明らかになることにより、**広範で複雑なプロジェクト間の依存関係について、開発者の理解を促進するなど**についても期待されている。



出所）Linux Foundation ホームページ　https://www.linuxfoundation.jp/wp-content/uploads/2022/05/LFResearch_SBOM_Report-ja.pdf

1. 昨年度のタスクフォースにおける議論の振り返り

2. ソフトウェアの管理手法等に関する国外の状況

3. 令和4年度のSBOM実証イメージ

4. ノウハウ集、活用モデル、取引モデルのイメージ

5. スケジュール、討議事項

本日ご議論いただきたい事項

- 主に以下の点についてご意見等をいただきたく存じます。

- **実証の進め方について**
  - 実証設計（内容や実証の選択肢など）について、考慮漏れや他に検討すべき事項などはないか
  - ノウハウ集、活用モデル、取引モデルの策定・検討に当たり、実証で留意すべき事項などはないか
- **ノウハウ集、活用モデル、取引モデルについて**
  - ノウハウ集、活用モデル、取引モデルの各文書の項目について、他に盛り込むべき内容などはないか
  - 策定・検討に当たり、国外の状況など留意すべき事項などはないか
- **今年度の本タスクフォースの進め方について**
  - 開催時期やスケジュールについて、他に検討すべき事項などないか