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11月28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. 最近のインシデント事例

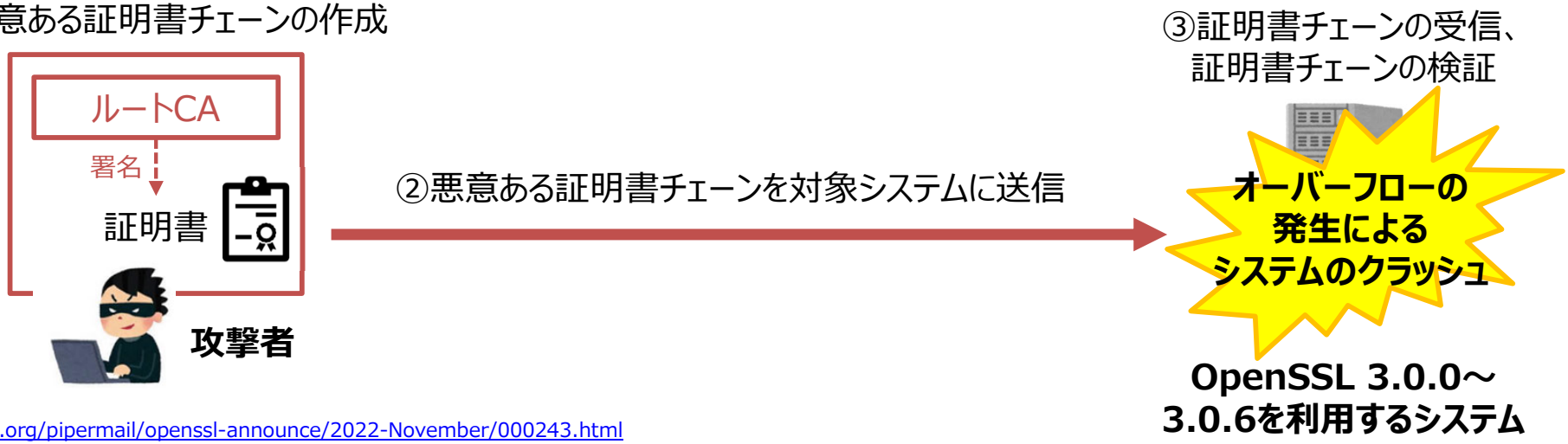
2. ソフトウェアの管理手法等に関する国内外の動向

3. SBOM実証の状況・課題等

OpenSSLの脆弱性：CVE-2022-3602、CVE-2022-3786

- 2022年10月25日、OpenSSL Projectは、SSL/TLSプロトコルのOSSライブラリである**「OpenSSL 3.0.0～3.0.6」の脆弱性に関する情報を発表**した。
- 本脆弱性は、OpenSSLのX.509証明書の検証処理に起因する脆弱性であり、悪用された場合、**システムがクラッシュする可能性**があるほか、**環境によってはリモートから任意コードを実行される可能性**がある。ただし、これらの問題は証明書チェーンの署名検証の後で発生するため、**悪意のある証明書に対して認証局(CA)が署名し、その後の処理が継続してしまう場合においてのみ悪用可能**であるため、**悪用可能性は限定的**である。
- OpenSSL Projectは、**当該脆弱性を修正した「OpenSSL 3.0.7」を2022年11月1日に公開**し、利用者に対して、脆弱性対応のための迅速なアップデートを促した。
- なお、10月25日の情報発表時点では、1つの脆弱性の深刻度を「Critical」と位置づけていたが、近年のOSの多くでスタックオーバーフロー保護が有効化されていることを踏まえ、評価が「High」に引き下げられた。
- 11月1日時点で、OpenSSL ProjectやJPCERT/CCは、**本脆弱性の悪用は確認していない**としている。

◆ **CVE-2022-3602、CVE-2022-3786を悪用した攻撃のイメージ**



https://mta.openssl.org/pipermail/openssl-announce/2022-November/000243.html
https://www.jpcert.or.jp/at/2022/at220030.html
https://jvn.jp/vu/JVNVU92673251/
https://securitylabs.datadoghq.com/articles/openssl-november-1-vulnerabilities/

1. 最近のインシデント事例

2. ソフトウェアの管理手法等に関する国内外の動向

3. SBOM実証の状況・課題等

【米国】ソフトウェアサプライチェーンの確保に関する覚書の発行

- 2022年9月14日、OMBは、**安全なソフトウェア開発手法の実装を通じたソフトウェアサプライチェーンの確保に関する覚書を発行**した。
- 各省庁等の機関に対して、本覚書発行後一定期間内に、**機関が使用するソフトウェアの目録作成**や、**NISTのガイダンスに基づく自己適合証明書をソフトウェアベンダーに要求すること**などが求められている。
- なお、**SBOMに関しては、適合証明のために必要に応じてソフトウェアベンダーからSBOMを入手することができるとして推奨の位置付け**としている。

覚書の概要

機関※は、安全なソフトウェア開発手法（SSDF）の実装を証明できるソフトウェアベンダーが提供するソフトウェアのみを使用すべきである。そのために、各機関の最高情報責任者（CIO）は、OMB及び最高調達責任者（CAO）と連携し、ソフトウェアベンダーによるSSDFの実装、実装の適合性を確保しなければならない。このために、機関は以下を実施する必要がある。

1. **機関は、ソフトウェア使用前に、SSDFの実装の適合性を証明する自己適合証明書の取得をソフトウェアベンダーへ要求する。**
2. **機関は、必要に応じて、自己適合証明書に付随する成果物（SBOM等）をソフトウェアベンダーから入手することができる。**

■ 対象ソフトウェア：
ファームウェア、OS、アプリケーション、アプリケーションサービス（クラウドベースのソフトウェア）、ソフトウェアに使用されるOSS、ソフトウェアを使用する製品
※ 機関によって開発されたソフトウェアや直接的に入手したOSSは対象外

■ 要件の適用範囲：
覚書発行日以降に開発されたソフトウェア（既存ソフトウェアのメジャーバージョンアップ含む）を機関が使用する場合に適用される。

※ 44 U.S.C. § 3502(1)で定義される「機関（Agency）」で、連邦政府、軍関係省、行政法人、行政管理法人、政府行政部門のその他施設（大統領府を含む）、独立規制機関が対象。

覚書発行日以降の各機関の主な対応スケジュール

各機関

＜覚書発行後90日以内＞
- 対象となる全てのソフトウェアの目録を作成
  ※「重要なソフトウェア」は別の目録を作成

＜覚書発行後270日以内＞
- 「重要なソフトウェア」の自己適合証明書を取得

＜覚書発行後365日以内＞
- 全てのソフトウェアの自己適合証明書を取得

OMB

＜覚書発行後90日以内＞
- 各機関が、本覚書の適用を延長・免除するための申請方法を専用WEBサイトへ掲載

＜覚書発行後180日以内＞
- CISA、GSAと協議し、機関間で保護及び共有する仕組みを備えた、自己適合証明書や付随する成果物を管理するためのリポジトリ要件を確立

CISA

＜覚書発行後120日以内＞
- OMBと協議し、文書業務削減法（PRA）に準拠した、自己適合証明書の共通様式を制定

＜OMBによるリポジトリ要件の確立から1年以内＞
- GSA、OMBと協議し、自己適合証明書や付随する成果物を管理するリポジトリのためのプログラム計画を策定

出所）OMB, ” Enhancing the Security of the Software Supply Chain through Secure Software Development Practices”
https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf

【米国】連邦政府のOSS利用におけるセキュリティ確保のための法案

- 2022年9月、**連邦政府のOSS利用におけるセキュリティ確保に向けた法案が米国上院へ提出**された。
- 本法案では、OSS利用におけるセキュリティ確保には特徴的な課題が存在するとし、**国土安全保障法（合衆国法典 Title 6）に対して、OSSのセキュリティに関する内容の加筆を要求**している。
- 加えて、**CISAに対して、OSS利用におけるセキュリティ確保における責任の明確化、OSSのリスクを評価するためのフレームワークの公開、各省庁に向けたOSSに関するガイダンスの発行を要求**している。
- また、**CISAに選定された機関に対しては、機関内にオープンソースプログラムオフィス（OSPO）の設立が要求**されている。

本法案の要求事項の概要

オープンソース ソフトウェアの セキュリティ義務（Section 3）	✓ 国土安全保障法第22編（合衆国法典 Title. 6 §651）の副題Aを以下のとおりに改正すること。 • 第2201条（合衆国法典 Title. 6 §651 ）において、OSSという用語の定義を追加する。 • 第2202条(c) (合衆国法典 Title. 6 §652(c))において、CISAの責任として「各省庁におけるソフトウェア開発ライフサイクルにおける、OSSを含むソフトウェアの安全な使用を支援」を追加する。 • 末尾に、「第2220条 E. OSSセキュリティの責任」を追加する。具体的には、CISAは主に以下の取組に責任を持つ。 ➢ OSSに関する各省庁の取組の支援、OSSに関する公的な窓口、OSSの脆弱性情報の開示を支援することによるサプライチェーンのセキュリティ確保の支援を実行する。 ➢ 本条の制定日から1年以内に、OSSのリスクを評価するためのフレームワーク（OSS内のコードのセキュリティ情報、OSSにパッチが適用されていない脆弱性の数と重大度等の評価観点や基準）を公開し、適宜更新する。 ➢ 上記のフレームワーク公開後、1年以内に、各省庁が使用しているOSSを対象にリスクを評価する。
ソフトウェア・セキュリティ アドバイザリー委員会（Section 4）	✓ 国土安全保障法第2219条(d)(1)（合衆国法典 Title. 6 §665 e(d)(1)）を以下のとおり改正すること。 • サイバーセキュリティ問題に対処するための小委員会の議題として、「OSSセキュリティを含むソフトウェアセキュリティ」を追加する。
オープンソース ソフトウェアガイダンス（Section 5）	✓ CISAは、本法案制定日から1年以内に、各省庁に向けたOSSに関するガイダンス（OSSの安全な利用やOSSへの貢献をどのように実現するか等）を発行すること。 ✓ CISAによって選定された機関は、本法案制定日から1年以内に、OSSの安全な使用やリスク管理等を実行する試験的なオープンソースプログラムオフィス（OSPO）を設立すること。

出所）Congress.gov, ”S.4913 - Securing Open Source Software Act of 2022”
https://www.congress.gov/bill/117th-congress/senate-bill/4913/text

（参考）OSPO（Open Source Program Office）の概要

- OSPO（Open Source Program Office）とは、**OSS活用環境の整備、関連部署とのOSS活用における連携、OSSコミュニティとの連携等、OSS関連活動を支援する社内組織のこと**である。
- OSPOを導入することで、組織のオープンソース戦略に従った効果的・効率的なOSS利活用が可能となり、これにより、**製品品質の向上、適切なライセンスの管理、外部コミュニティとの連携活性化**等が期待される。
- 海外ではGAFAM、Cisco、Intel等の企業がOSPOを擁しているほか、国内ではソニーグループ、富士通、メルカリ、サイバートラスト等において、OSPOが設置されている。
- Linux Foundation及びその傘下のTODOグループは2022年2月にホワイトペーパーを発表し、**OSPOの共通的特徴、OSPOの組織成熟度モデル、OSPOを特徴づける6つの原型**を示した。
- 関連する国内の取組として、**OpenChain Japan WGに設立されたOSPOに関するサブグループ**では、**日本企業におけるOSPOのあるべき姿を検討**しつつ、**その実現に資する成果物の作成を目標に活動**している。

Linux Foundation・TODOグループが示したOSPOの共通的特徴

- 社員が、OSSの使用を促進され、教育されたもとで業務遂行している
- その組織が、OSSの使用や稼働に関して正式なポリシーを持っている
- エグゼクティブたちが、OSSおよび、より広い意味での「オープンソース」が重要な戦略的資産であることを認識している
- 多くの社員がオープンソースプロジェクトにコードをコントリビュートしている
- オープンソース(へ)の消費や参加を合理化し促進するためのプロセス、手順、ツールが整備されている

Linux Foundation・TODOグループが示したOSPOの組織成熟度

OSPOの成熟度（ステージ）	概要
ステージ0 **オープンソースのアドホックな採用**	OSSを活用しているが、管理組織はなく、オープンソース戦略も存在していない状態
ステージ1 **OSSコンプライアンス、インベントリ、および開発者教育の提供**	OSS活用による法的リスクやライセンス情報を管理しつつ、ソフトウェアインベントリ (SBOM)の取得や開発者の教育を行っている状態
ステージ2 **OSSの使用とエコシステムへの参加の啓発**	OSS活用による経済的なメリットを実現し、OSSコミュニティとの交流を深めつつ、OSS関連活動の仕組みを構築した状態
ステージ3 **OSSプロジェクトのホストとコミュニティの育成**	OSSプロジェクトを1から立ち上げ、ホスト役や主要スポンサーとして活動しつつ、コミュニティを育成する状態
ステージ4 **戦略的意思決定のパートナー化**	技術的意思決定の戦略的パートナーとなり、OSSプロジェクトのベンチマーク等をリードする状態

（出所）TODOグループ、Open Source Program Office (OSPO)の進化　−Bloomberg、Comcast、Porsche 各社ケーススタディから見るOSPOの成熟モデル−
https://www.linuxfoundation.jp/wp-content/uploads//2022/08/LFResearch_OSPO_Report-jp.pdf

【EU】EUサイバーレジリエンス法（草案）の発表　1/2

- 欧州委員会は2022年9月、**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。**本法案では、**デジタル製品を上市する際のルール**、**製品におけるサイバーセキュリティに関する要求事項**、**製造業者に課される脆弱性対応の要求事項**、**当該要求事項への順守を担保するための市場監督者へのルール**を規定。
- 本法案の対象製品について、例外を除き、**あらゆるデジタル製品が対象**であり、**SBOM作成や製品に対するセキュリティ要件への適合性証明（自己適合宣言又は第三者認証）を要求**。
- 製造業者が本法案のセキュリティに関する要件を遵守にしない場合、**罰金あり**（最大1,500万ユーロ又は前会計年度の世界全体の総売上高の最大2.5%のいずれか高い方）。
- 本法案は**2023年後半の発効**、**2025年後半（発効から2年後）の適用**を目指しているが、**製造業者における脆弱性の報告義務は2024年後半（発効から1年後）からの適用**を位置づけている。

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。

▶ **自己適合宣言か第三者認証を選択**

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。
例）産業用以外のルーター・スイッチ、VPN装置、SIEMなど。

▶ **EUCCやEN規格の対象外の製品は第三者認証が必要**

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。
例）産業用ルーター・スイッチ、産業用制御システム、PC用のOSなど。

▶ **第三者認証が必要**

対象外となる製品：
既存のEU法により要求事項が課されている製品などは対象外

（例）
- 医療機器
- 体外診療用医療機器
- 自動車
- 航空機関連機器
- SaaSなどのソフトウェアサービス
- 研究開発目的のOSS　等

出所）EU, Cyber Resilience Act https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

【EU】EUサイバーレジリエンス法（草案）の発表　2/2

- 法案では、対象製品に対する要求事項として、**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**や、**悪用可能な既知の脆弱性がない状態で提供すること**を要求。
- また、製造業者に対する要求事項として、デジタル製品の脆弱性ハンドリングに関する要求事項、製品のセキュリティ評価に関する要求事項、利用者への情報提示に関する要求事項、製品の適合性評価に関する要求事項、脆弱性の報告義務に関する要求事項のほか、**SBOMやOSS管理に係る要求事項も規定**。
- 具体的には、**製品のトップレベルの依存関係を網羅した機械判読可能なSBOMの作成**を求めているほか、**外部コンポーネントの脆弱性に関する情報共有手段の確立**や**使用しているコンポーネントに脆弱性が見つかった場合の報告**についても要求しており、また、**SBOMの様式や要素は、欧州委員会が実装法令によって規定できる**としている。

EUサイバーレジリエンス法の要求事項のうち、SBOMやOSS管理に係る要求事項（抜粋）

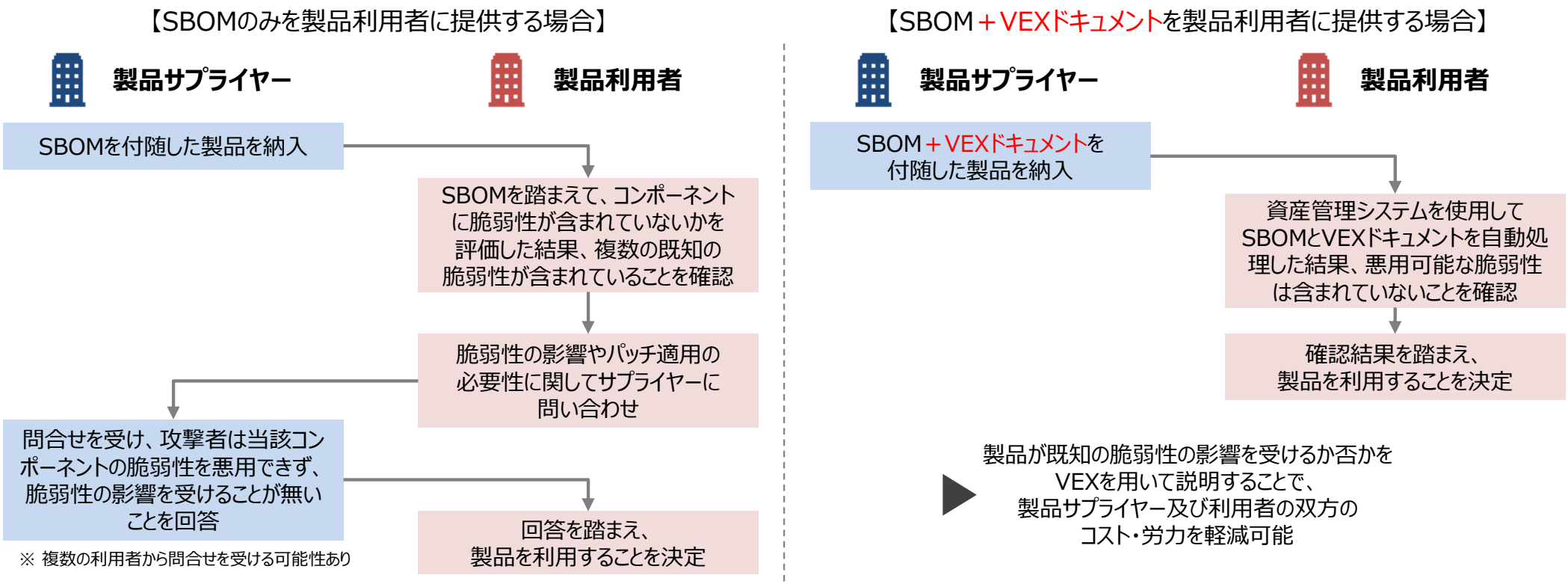
要求対象	SBOMやOSS管理に係る具体的な要求事項（抜粋）
デジタル製品に対する要求事項	• デジタル製品は、リスクに応じた適切なレベルのサイバーセキュリティを確保するように設計、開発、生産すること。 • デジタル製品は、悪用可能な既知の脆弱性がない状態で提供すること。
製造業者に対する要求事項	• デジタル製品の製造者は、製品に含まれる脆弱性とコンポーネントを特定し、文書化しなければならない。これには、少なくとも製品のトップレベルの依存関係を網羅する、一般的に使用され機械判読可能な形式のソフトウェア部品表を作成することが含まれる。 • 製造業者は、デジタル製品およびその製品に含まれる第三者のコンポーネントの潜在的な脆弱性に関する情報の共有を促進するための手段を講じなければならない。（デジタル製品で発見された脆弱性を報告するための連絡先を提供することを含む） • 製造業者は、オープンソースコンポーネントを含む、デジタル製品に組み込まれたコンポーネントの脆弱性を特定した場合、そのコンポーネントを保守する個人または団体に報告しなければならない。

出所）EU, Cyber Resilience Act https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

VEXとは

- Vulnerability Exploitability eXchange（VEX）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つ**であり、米国NTIAを中心として開発された。
- VEXの主な目的は、製品利用者に対して、**製品が特定の脆弱性の影響を受けるかどうか**、そして**影響を受ける場合に是正するために推奨されるアクションがあるかどうかの追加情報を提供**し、**製品サプライヤー及び利用者の双方のコスト・労力を軽減すること**にある。
- VEXは、**SBOMを活用した脆弱性管理をより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。

VEXを導入することのメリットの例



出所）NTIA, "Vulnerability Exploitability eXchange(VEX) – An Overview" https://www.ntia.gov/files/ntia/publications/vex_one-page_summary.pdf
NTIA, "Framing Working Group" https://www.ntia.doc.gov/files/ntia/publications/framing_2021-04-29_002.pdf

【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。

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文書の識別文字列 • VEX文書の作成者 • VEX文書の作成者の役割 • VEX文書のタイムスタンプ
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）CSAFの概要

- CSAF（Common Security Advisory Framework）とは、標準化団体OASIS Openが開発した**JSONベースの機械判読可能なセキュリティアドバイザリー標準**のことで、**動的に変動する製品のセキュリティアドバイザリー情報を効率的に自動処理する目的で開発**された。
- **VEXは、CSAFの1つのプロファイルとして実装**されている。
- CSAFはメタデータに関するプロパティ（document）、アドバイザリーの対象となる製品に関するプロパティ（product_tree）、脆弱性に関するプロパティ（vulnerabilities）の3つに分かれ、記述される。
- Schneider Electric社など一部の海外企業では、既にCSAF形式でのアドバイザリー情報提供を始めている。

CSAFフォーマットの3つのプロパティ

document

セキュリティアドバイザリーに関するメタデータが記述される（色付き下線は必須オブジェクト）：

- 謝辞（acknowledgments）
- 統合的な深刻度（aggregate_severity）
- カテゴリ（category）
- CSAFバージョン（csaf_version）
- 配布範囲（distribution）
- 言語（language）
- ノート（notes）
- 発行者（publisher）
- 参考情報（references）
- ソース言語（source_lang）
- タイトル（title）
- 来歴（tracking）

product_tree

セキュリティアドバイザリーの対象製品のベンダー、バージョン、名称、ID等を、ブランチ（branches）の項目に基づき、木構造で記述される。

記載例

```
"product_tree": {
  "branches": [
   {
    "name": "Cisco",
    "category": "vendor",
    "branches": [
     {
      "name": "IOS",
      "category": "product_name",
      "branches": [
       {
        "name": "12.2SE",
        "category": "product_version",
        "branches": [
    ....
```

vulnerabilities

1つ以上の脆弱性に関するオブジェクトが記述される：

- 謝辞（acknowledgments）
- CVE番号（cve）
- CWE情報（cwe）
- 検出日（discovery_date）
- フラグ（flags）
- 脆弱性ID（ids）
- 関与（involvements）
- ノート（notes）
- 製品ステータス（product_status）
- 参考情報（references）
- 発表日（release_date）
- 改善策（remediations）
- スコア（scores）
- 脅威（threats）
- タイトル（titles）

出所）OASIS, Common Security Advisory Framework Version 2.0 https://docs.oasis-open.org/csaf/csaf/v2.0/csaf-v2.0.html
Schneider Electric, Cybersecurity Support Portal https://www.se.com/ww/en/work/support/cybersecurity/security-notifications.jsp
OASIS GitHub Repositories for TC Work, https://github.com/oasis-tcs/csaf/blob/master/csaf_2.0/examples/csaf/cisco-sa-20180328-smi2.json

（参考）CSAF形式のVEXドキュメントの構造

- **CSAFの3つのプロパティに基づきVEXドキュメントは記述される**。
- メタデータに関するプロパティ（document）では、発行者、タイトル、ID、初回発行日、改訂履歴、VEXドキュメントのステータス等、当該VEXドキュメントに関する情報が記述される。
- 製品に関するプロパティ（product_tree）では、ベンダー、製品名、バージョンの関係性をツリー構造が記述される。
- 脆弱性に関するプロパティ（vulnerabilities）では、各製品・各バージョンに存在する脆弱性について、4つの脆弱性ステータスのどれに該当するかが記述される。
- CSAF形式のVEXドキュメントを作成・編集するツールとしては、ドイツBSIが開発したSecvisogram※が存在。

VEXドキュメントの構造（3つのプロパティの概要とプロパティの関係）

※ https://github.com/secvisogram/secvisogram

document

VEXドキュメントに関するメタデータが記述される。

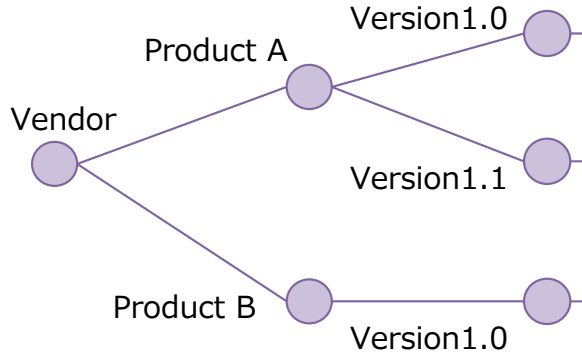
- カテゴリ（category）
- CSAFバージョン（csaf_version）
- 発行者（publisher）
- タイトル（title）
- ドキュメントID（id）
- 初回発行日（initial_release_date）
- 改訂履歴（revision_history）
- VEXドキュメントのステータス（status）
- VEXドキュメントのバージョン（version）

等

product_tree

製品ベンダー、製品名、バージョンごとに分岐し、最終的に製品を特定する製品IDで終了する。

製品IDは、その製品と脆弱性を関連付けるために使用される。製品IDには、CPE、ファイルハッシュ、purl、SBOMのURLなどを付け加えることで、製品特定の曖昧さを防止することが可能である。



vulnerabilities

脆弱性ごとに、各製品・バージョンが4つの脆弱性ステータスのどれに当てはまるかが記述される。

製品が脆弱性の影響を受ける場合（known_affected）、リスク軽減に関する情報（remediations）を含めることが可能である。

CVE-2021-44228

“known_affected”

＋ “remediations”

“known_not_affected”

CVE-2021-XXXXX

“known_not_affected”

・・・

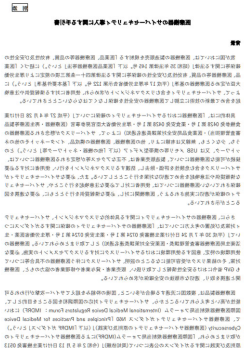
出所）aDolus Technology Inc, ”Understanding Vulnerability Exploitability eXchange (VEX)”
https://adolus.com/solutions/vulnerability-management/

【国内】ソフトウェア管理手法等に関する動向

- 日本においても、手引書にSBOMに関連する対策が明記されるなど、国内においてもSBOMが少しずつ認識され始めつつある。

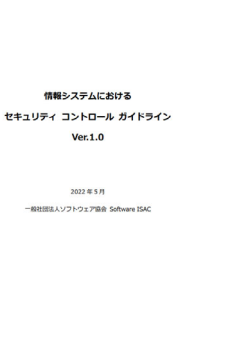
「医療機器のサイバーセキュリティ導入に関する手引書」の公表（2021年12月、厚生労働省）

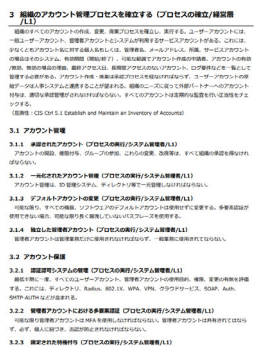
- 医療機器の製品ライフサイクル全体を通じてセキュリティリスクを提言するために、IMDRFガイダンスの要求事項を踏まえて策定された文書で、SBOMに関する内容も含まれる。
- なお、厚生労働省は、2023年を目処に医療機器に対するSBOM要求に関する基準等の改正を予定している。



「情報システムにおけるセキュリティコントロールガイドライン Ver.1.0」の公表（2022年5月、Software-ISAC）

- システム運用のライフサイクルを通じて必要な、セキュリティの管理策をまとめたガイドライン。
- SBOMに関して、アプリケーションのSBOMを作成し、定期的に更新することの重要性が明記されているほか、サプライチェーン全体でのSBOM管理の重要性も触れられている。


情報システムにおける
セキュリティ コントロール ガイドライン
Ver.1.0
2022 年 5 月
一般社団法人ソフトウェア協会 Software ISAC



「Open Source Security Summit Japan」の開催（2022年8月、Linux Foundation/OpenSSF）

- 2022年5月にホワイトハウスで開催されたSummitに続くもので、OSSのセキュリティ課題とこれを向上する方法に関して議論を行った。
- 国内からは、日立製作所、富士通、トヨタ等の企業のほか、経済産業省、IPA、JPCERT/CCの政府関係機関も参加。

（出所）厚生労働省、Software-ISAC、Linux Foundation

1. 最近のインシデント事例

2. ソフトウェアの管理手法等に関する国内外の動向

3. SBOM実証の状況・課題等

実証の実施体制等

● 実証の目的や産業分野ごとの法制度等を考慮し、以下の実施体制等により実証を継続中。

● 実証の目的および成果目標

– 産業分野ごとのリスク、法制度に応じて、SBOMを用いた部品のリスク管理を効果的に行うための方法についてコスト・効果の比較評価を行い、現実的な適用範囲と課題について整理する。
– 実証を通じて、SBOM導入ノウハウ集、SBOMの適用範囲を例示するSBOM活用モデル、取引契約の例示によりSBOM導入を促進するSBOM取引モデルのコンテンツ要素（一部）を作成することを目的とする。
– 法的な要件化が進む医療機器分野、自動車分野および、効果が期待できるソフトウェア分野について、実ソフトウェアに対するサプライチェーンを考慮した体制により、評価を行う。

実施体制等（実証の実施者・関係者及び対象製品など）

分野	関連する業界団体	実証実施企業及び関係企業など					関連法制度・基準等	対象製品
		ユーザ	最終ベンダ（製販業者、インテグレータ等）	ティア1サプライヤ	ティア2サプライヤ	サードパティサプライヤ		
医療機器	日本医療機器産業連合会	法人（ヒアリング協力予定：大学病院）	近畿レントゲン工業（製販業者）	ライフサイエンスコンピューティング		Microsoft, google等	(厚労省) 医療機器サイバーセキュリティ手引書 (国際) IMDRF追補ガイダンス (米国) FDA ガイダンス	歯科用CT
自動車	（日本自動車工業会）	個人	トヨタ自動車（OEM）	東海理化	サニー技研	OSSベンダ等	(国交省)道路運送車両の保安基準 (国際)UN-R155, 156 (米国)NHTSAガイダンス	自動車ヒーターコントローラ
ソフトウェア	ソフトウェア協会	法人（ヒアリング協力）	トレンドマイクロ、さくらインターネット、コラボスタイル（製販業者、インテグレータ）			Adobe, Amazon, Microsoft等	(米国)NISTサプライチェーンガイダンス, FedRAMP	ネットワーク脅威検知ソフトなど

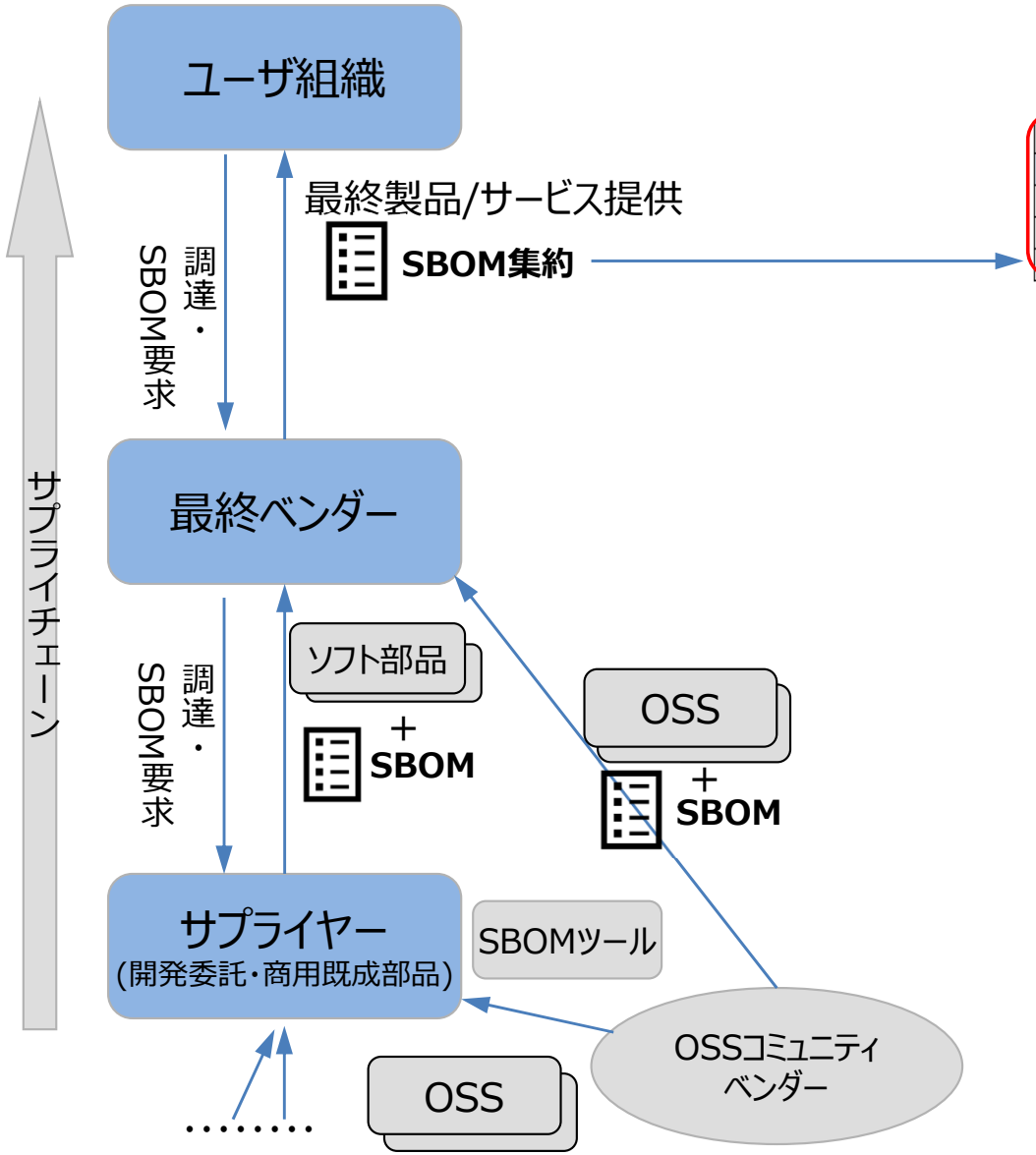
これまでに実証で確認された課題と取組みの方向性

これまでに確認された課題は、ノウハウ集等への記載の検討や引き続き実証において整理等することを検討。

区分	これまでに確認された課題等（確認された分野など）	対応方針
技術・ツール	SBOMツールを単に適用しただけでは、サードベンダ製品におけるソフトウェア部品など特定されないケースが多数存在。**（ソフトウェア分野）**	ツールの留意点などを整理しつつ、サードベンダからのSBOMの提供に係る課題やノウハウなどを整理
	実際に含まれる部品のうちどの程度SBOMを生成できるかにより、脆弱性管理の範囲は大きく異なる。OSSなど再帰的な部品のSBOMを完全に生成するためには、膨大なコストがかかる。**（ソフトウェア分野）**	実証を通じたSBOMの現実的な網羅範囲の整理し、活用モデルで妥当な範囲を例示するなど
	SBOMにおけるソフトウェア部品の一意性を確保した運用が行われていないため、脆弱性情報とのマッチングが難しい。**（共通）**	脆弱性情報と関連したソフトウェア部品名称の記載などSBOMにおける記載の仕方の整理
	対象システムの全体像が把握できていないため、SBOMツール適用範囲を適切に設定できず、全体のリスクが管理できていない。**（共通）**	使用しているソフトウェアの管理の必要性などをノウハウ集等へ記載
	異なるSBOMツール間でのSBOMの共有が困難。ツールにより対応する機能が異なるなど、ツール選定時に機能面や価格面などの判断が必要。**（共通）**	ツールを利用する際の留意事項として整理し、ノウハウ集等へ記載
	脆弱性に対して、悪用可能性情報を把握できない可能性があり、不具合報告の判断が難しい。**（医療機器分野）**	VEXなど、脆弱性判断に係る情報の活用等を検討
組織・取引	分野によっては厳格な部品管理が求められるが、中小企業などについてはSBOMに対する十分な理解や対応が現状できていない。**（共通）**	ノウハウ集の策定、企業への普及・啓発など
	SBOM生成・活用のコストの負担者が明確ではない。**（自動車分野）**	実証等で整理しつつ、取引モデルにおいて参考例を提示するなど
法制度	制度上の基準に対して、具体的なガイド改定中で、明確になっていない。**（医療機器分野）**	所管省庁など関係機関への実証結果のフィードバック

SBOMにおけるソフトウェア名称などの記載に係る課題

- SBOMの共有にあたり、SBOMの表記ゆれなどが課題。また、受け取り側において、SBOMを用いた脆弱性対応も踏まえ、検討が必要。



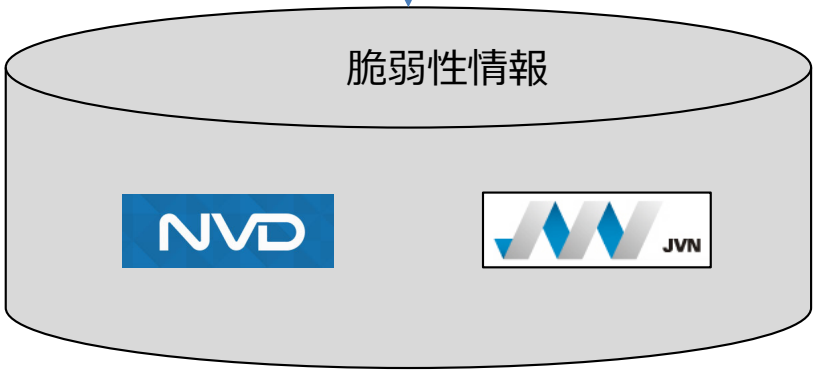
集約されたSBOM

コンポーネント	サプライヤー	バージョン	作成者	ハッシュ	ID	依存関係	関係性アサーション
Application	Acme	1.1	Acme	0x123	234	Self	Known
|--- Browser	Bob	2.1	Bob	0x223	334	Included in	Partial
|--- Compression Engine	Carol	3.1	Acme	0x323	434	Included in	Root
|--- Buffer	Bingo	2.2	Acme	0x423	534	Included in	Unknown

検討事項

・脆弱性情報との紐付けも見据え、SBOMの記載の仕方

・キー情報の設定など



以下、参考資料

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に基づくソフトウェア透明性の確保とリスク管理

- 脆弱性管理の効果は、SBOM生成・活用の範囲（カバレッジ）に影響を受けるが、SBOMの生成・活用を完全に実施することはコスト的に困難であるケースも多い。
- 分野ごとの制度や商慣習などに応じたレベルで、SBOMを生成・活用することによりサプライチェーンを通じたリスクの管理を実施できるよう、主なSBOM適用項目の選択肢を整理し、優先度の高い適用項目ごとのコスト・効果について計測・評価を実施する。

【SBOM作成等に係る主な適用項目】

	適用区分	主な適用項目（選択肢）
生成・共有	(a)SBOM作成主体 (Who)	(a1)自社
		(a2)サプライヤ（開発委託先）取引契約あり
		(a3)サプライヤ（サードパーティ）取引契約なし
	(b)依存関係 (What, Where)	(b1)直接利用部品※1（開発主体が直接利用する部品）
		(b2)間接利用部品※2（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）
	(c)生成手段(精査) (How)	(c1)手動で特定（構成管理情報利用）・ツールで生成
		(c2)ツールで特定・生成・誤検知精査なし
		(c3)ツールで特定・生成・誤検知精査あり
		(c4)開発委託元が、開発委託先の作成したSBOMを独立に検査
	(d)データ様式・項目 (What)	(d1)標準フォーマット（SPDX、CycloneDX、SPDX Lite等）
		(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
		(d3)上記を満たさない要素
活用	(e)活用範囲 (Why)	(e1)脆弱性の特定
		(e2)脆弱性の深刻度評価
		(e3)脆弱性の悪用可能性等の評価と対処
		(e4)ライセンス特定
	(f)活用主体 (Who)	(f1)製品利用者
		(f2)最終製品ベンダー
		(f3)各部品の開発者

実証等を踏まえ、対応レベルに応じて色分け

【SBOM適用範囲の整理】

SBOM作成主体	作成範囲	生成方法	生成項目	活用法
(a1)自社	(b1)直接利用部品	(c1)手動で特定（構成管理情報利用）・ツールで生成	(d1)標準フォーマット（SPDX、SPDXLite等）	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
			(d3)上記の一部のみ	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
		(c2)ツールで特定・生成・誤検知精査なし	(d1)標準フォーマット（SPDX、SPDXLite等）	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
		(c3)ツールで特定・生成・誤検知精査あり	(d1)標準フォーマット（SPDX、SPDXLite等）	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
		(c1)手動で特定（構成管理情報利用）・ツールで生成	(d1)標準フォーマット（SPDX、SPDXLite等）	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
(a2)サプライヤ（開発委託先）取引契約あり	(b1)直接利用部品	(c1)手動で特定（構成管理情報利用）・ツールで生成	(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
		(c2)ツールで特定・生成・誤検知精査なし	(d1)標準フォーマット（SPDX、SPDXLite等）	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
		(c3)ツールで特定・生成・誤検知精査あり	(d1)標準フォーマット（SPDX、SPDXLite等）	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
		(c1)手動で特定（構成管理情報利用）・ツールで生成	(d1)標準フォーマット（SPDX、SPDXLite等）	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
			(d2)大統領令最小要素を含む	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
			(d3)上記を満たさない要素	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価
			(d1)標準フォーマット（SPDX、SPDXLite等）	(e1)(e2)脆弱性・ライセンスの特定 (e3)(e4)悪用可能性・深刻度の評価

- SBOM生成・活用範囲（カバレッジ）は、SBOM適用項目選択肢の組み合わせとして整理を検討。
- 実証を通じて、比較可能な部分について、選択肢の範囲について参考情報などを提示する。