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3年10月29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. サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）とその実装へ向けた取組の方向性

2. 最近のインシデント事例

3. ソフトウェア管理等に関する諸外国の取組状況

4. 本タスクフォースにおける検討事項

（１）国内でのSBOM活用促進に向けた実証

（２）OSS管理手法に関する事例集の拡充

分野別SWGにおけるサイバー・フィジカルセキュリティ対策フレームワーク（CPSF）の具体化 とテーマ別TFにおける検討

- **6つの産業分野別サブワーキンググループ(SWG)**を設置し、CPSFに基づくセキュリティ対策の具体化・実装を推進
- 分野横断の共通課題を検討するために、3つの**タスクフォース（TF）を設置**

産業サイバーセキュリティ研究会ＷＧ１（制度・技術・標準化）

標準モデル（CPSF）

Industry by Industryで検討
(分野ごとに検討するためのSWGを設置)

- **ビルSWG**
  - ガイドライン第1版の策定(2019.6)
- **電力SWG**
  - 小売電気事業者ガイドライン策定(2021.2)
- **防衛産業SWG**
- **自動車産業SWG**
  - ガイドライン1.0版を公表(2020.12)
- **スマートホームSWG**
  - ガイドライン1.0版を公表(2021.4)
- **宇宙産業SWG**
  - 2021年3月に第2回を開催
- ・・・

分野横断SWG

『第3層』TF：『サイバー空間におけるつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース

検討事項：
データの信頼性確保に向け「データによる価値創造（Value Creation）を促進するための新たなデータマネジメントの在り方とそれを実現するためのフレームワーク（仮）」骨子案のパブリックコメントを実施。

ソフトウェアTF：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

検討事項：
OSSの管理手法に関するプラクティス集の策定、SBOM活用促進に向けた実証事業（PoC）を検討。

『第2層』TF：『フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース

検討事項：
フィジカル空間とサイバー空間のつながりの信頼性の確保するための「IoTセキュリティ・セーフティ・フレームワーク(IoT-SSF)」を公開。

1. サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）とその実装へ向けた取組の方向性

2. 最近のインシデント事例

3. ソフトウェア管理等に関する諸外国の取組状況

4. 本タスクフォースにおける検討事項

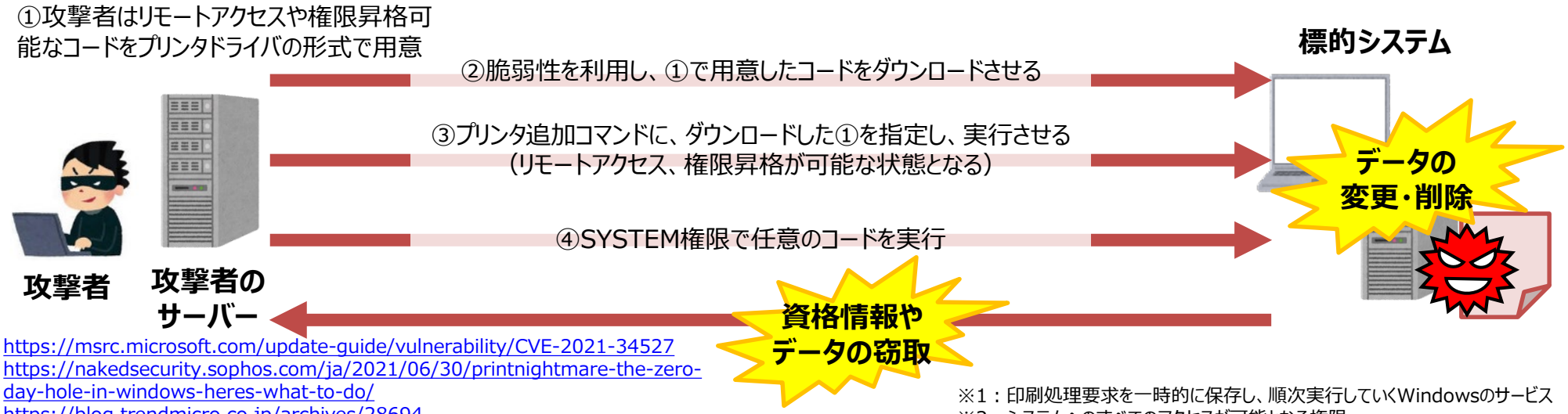
（１）国内でのSBOM活用促進に向けた実証

（２）OSS管理手法に関する事例集の拡充

Windows 印刷スプーラーサービスの脆弱性：PrintNightmare

- 2021年6月、Windows・Windows Server製品の印刷スプーラーサービス※1の脆弱性が発表され、PrintNightmareと命名された。
- 悪用された場合、**SYSTEM権限※2 で任意のコードが実行され、データの変更や削除、アカウント情報の窃取が行われる可能性**がある。
- Microsoft社が2021年6月に権限昇格の脆弱性に対する更新プログラムを公開したところ、**外部研究者が**リモートコード実行の脆弱性へのパッチも含まれていると誤解し、**リモートコード実行に関する概念実証コードを公開**した。
- これを受け、Microsoft社は、2021年7月にリモートコード実行の脆弱性に対する更新プログラムを緊急公開した。米国CISAも、リモートコード実行のリスクが高いものと判断し、**Windows・Windows Server製品を使用しているすべての連邦政府機関に対し、脆弱性に対処するよう緊急指令を発出**した。

◆攻撃イメージ

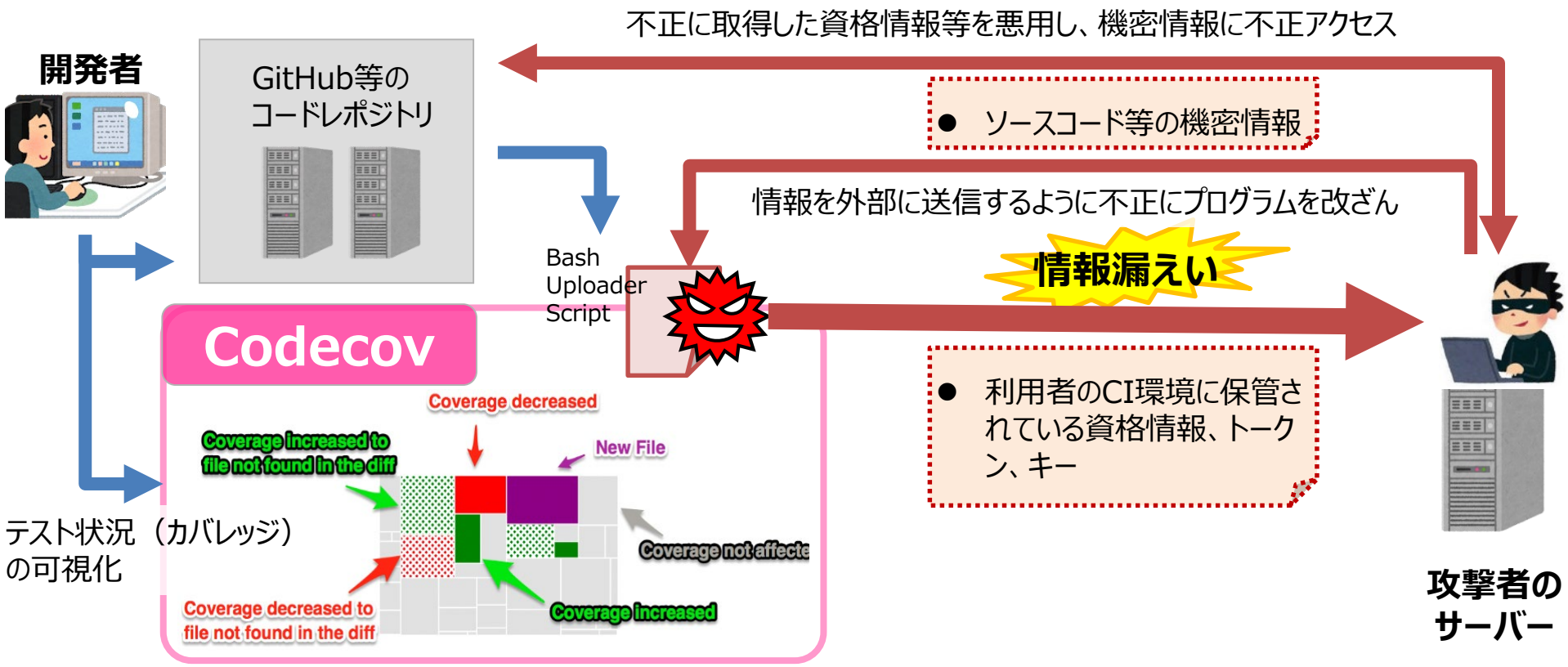


https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527
https://nakedsecurity.sophos.com/ja/2021/06/30/printnightmare-the-zero-day-hole-in-windows-heres-what-to-do/
https://blog.trendmicro.co.jp/archives/28694
https://cyber.dhs.gov/ed/21-04/

※1：印刷処理要求を一時的に保存し、順次実行していくWindowsのサービス
※2：システムへのすべてのアクセスが可能となる権限

ソフトウェア開発のテスト支援ツール”Codecov”にバックドア

- “Codecov”は、世界中で2.9万の組織、100万人以上に利用される（2021年4月時点）CI/CD(継続的インテグレーション／継続的デリバリー)を実現するためのテスト支援ツール。ソースコードのテスト状況を可視化する。
- 2021年4月、Codecovに含まれるBash Uploader Scriptが不正に書き換えられ、**利用者の資格情報等が不正に外部に送信され、ソースコードなどの機密情報が漏えいするリスクがある**ことが利用者指摘により発覚。
- Bash Uploader Scriptが書き換えられていた可能性があるのは2021年1月31日～2021年4月1日の期間であり、**不正取得された資格情報等が悪用され、国内でもソースコードや顧客情報の漏えい事案**が確認されている。

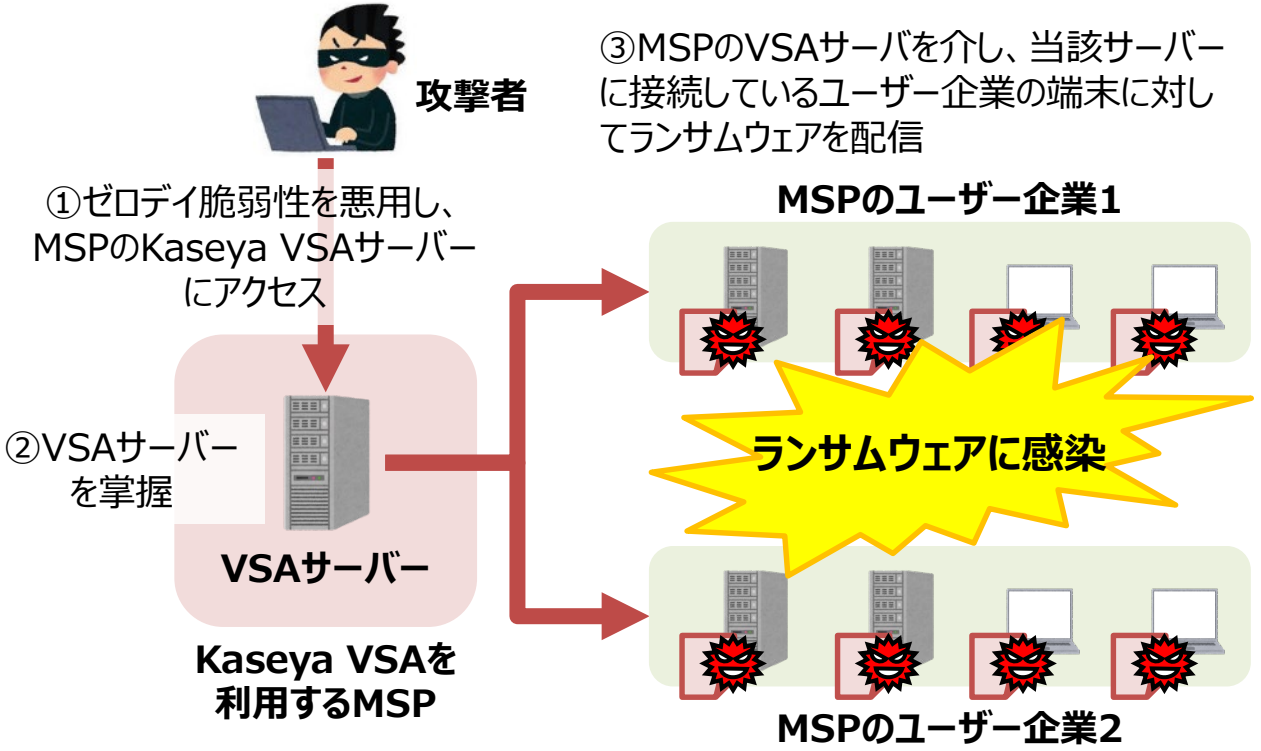


https://about.codecov.io/security-update/

Kaseya VSAの脆弱性を利用したサプライチェーンランサムウェア攻撃

- 2021年7月、米国のKaseya社は、同社のリモートIT管理サービス**「Kaseya VSA」をオンプレミスで利用している企業に対するランサムウェア攻撃が発生**していると発表した。
- Kaseya VSAはマネージドサービスプロバイダー（MSP）に導入されていることが多く、複数のMSPが攻撃を受けたことで被害範囲が拡大し、**攻撃を受けた可能性のあるユーザー企業は全体で1,500組織と推計**されている。
- CISAとFBIは、MSPとそのユーザー企業向けに対策ガイダンスを公開し、**MSPやそのユーザー企業に対して、ガイダンスに従ったセキュリティ対策を講じることを強く要請**した。

◆MSPへの攻撃とユーザー企業への影響のイメージ



◆CISA、FBIの対策ガイダンスの概要

MSP向けの推奨アクション

- Kaseya社により公開された侵入検出ツールをダウンロードし、IOCがシステム上に存在するかを確認する。
- 組織の管理下の全アカウントに対して多要素認証を有効にし、顧客向けサービスに対しても可能な限り多要素認証を有効にする。
- 通信許可リストを作成し、リモート監視・管理機能との通信を既知のIPアドレスに制限する。
- リモート管理の管理インターフェースをVPNまたは専用の管理ネットワーク上でFWよりも内部に配置する。

ユーザー企業向けの推奨アクション

- バックアップが最新であることを確認し、エアギャップされ、円滑に取得可能な場所に保管されていることを確認する。
- Keseya社の修正ガイダンスに従い、手動でのパッチ管理プロセスに戻し、修正パッチが利用可能になり次第、インストールを行う。
- 多要素認証、主要なネットワーク管理アカウントに対する最小特権の原則に基づいた実装を行う。

https://www.kaseya.com/potential-attack-on-kaseya-vsa/
https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks
https://us-cert.cisa.gov/ncas/current-activity/2021/07/04/cisa-fbi-guidance-msps-and-their-customers-affected-kaseya-vsa

1. サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）とその実装へ向けた取組の方向性

2. 最近のインシデント事例

3. ソフトウェア管理等に関する諸外国の取組状況

4. 本タスクフォースにおける検討事項

（１）国内でのSBOM活用促進に向けた実証

（２）OSS管理手法に関する事例集の拡充

【欧州】サプライチェーン攻撃に関するENISAレポート

- 2021年7月、ENISAは**24件のサプライチェーン攻撃事例に関する調査・分析結果を示すレポート**を公開した。
- また同月、調査・分析結果を踏まえ、**サプライチェーン攻撃に関する現状説明**や、**サプライヤー及び顧客（調達者）が実施すべき推奨事項をまとめたプレス発表**を行った。
- ENISAは、2021年には2020年の4倍のサプライチェーン攻撃が発生すると推定している。

サプライチェーン攻撃に関するENISAレポート・プレス発表の全体像

2020年1月から2021年7月にかけて発生した24件のサプライチェーン攻撃事例に関して、提案された分類法に基づき分類を行い、結果を調査・分析
（攻撃事例の例：SolarWindsの事例、Codecovの事例、Kaseyaの事例、Apple Xcodeの事例 等）

ENISAにより提案されたサプライチェーン攻撃の分類法

サプライヤーに対するサプライチェーン攻撃		顧客に対するサプライチェーン攻撃	
用いられる攻撃技術	攻撃対象	用いられる攻撃技術	攻撃対象
• マルウェア感染 • ソーシャル・エンジニアリング • ブルートフォース • ソフトウェア脆弱性の悪用 • コンフィグレーション脆弱性の悪用 • OSINT情報	• 既存のソフトウェア • ライブラリ • コード • コンフィグレーション • データ • プロセス • ハードウェア • 人員 • サプライヤー(組織)	• 信頼関係の悪用 • Web閲覧による感染 • フィッシング • マルウェア感染 • 物理的攻撃、改変 • 偽造、模倣品	• データ • 個人情報 • 知的財産 • ソフトウェア • プロセス • 処理能力 • 金銭 • 人員

主な調査・分析結果
- 50%の攻撃は有名なAPTグループにより実施された
- 62%の攻撃において、マルウェアが攻撃技術として採用
- 58%の攻撃がデータ（個人情報、知財等の顧客の情報）へのアクセスを目的としていた
- サプライヤーへの攻撃の66%は、サプライヤーのコードが対象
- 顧客への攻撃の62%は顧客とサプライヤーとの信頼関係を悪用

顧客が実施すべき主な推奨事項
- サプライヤーとサービスプロバイダーの特定、文書化
- 様々なタイプのサプライヤーやサービスのリスク基準を定義
- サプライチェーンリスクと脅威の監視
- 製品やサービスのライフサイクル全体にわたるサプライヤーの管理
- サプライヤーが共有／アクセス可能な資産・情報の分類と手順整備　等

サプライヤーが実施すべき主な推奨事項
- 製品、コンポーネント、サービスの設計、開発、製造、提供に使用されるインフラが、サイバーセキュリティのプラクティスに従っていることを確認
- 一般的に認められた製品開発プロセスに整合する製品開発、保守、サポートのプロセスを実施
- 社内外の情報源から報告されるセキュリティ脆弱性の監視
- パッチ関連情報を含む資産インベントリの維持　等

出所） ENISA, “Threat Landscape for Supply Chain Attacks” https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks
ENISA, “Understanding the increase in Supply Chain Security Attacks” https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks

【米国】ソフトウェア・サプライチェーンにおける利用者とベンダーの推奨事項

- 2021年4月、CISAは**ソフトウェア・サプライチェーンにおける推奨事項を示した文書を公開**した。
- ソフトウェア・サプライチェーンリスクの概要や事例を示すとともに、サプライチェーンリスクの特定・評価・軽減に向け、NISTの**C-SCRM（サイバーサプライチェーンリスク管理）プログラムやSSDF（セキュアソフトウェア開発フレームワーク）に基づき、ソフトウェアの利用者及びベンダーが実施すべき推奨事項**を示している。

ソフトウェア利用者が実施すべき推奨事項

ソフトウェアを調達し、利用する組織は、他のICT製品・サービスと同様に、**リスク管理プログラムに基づいたソフトウェアの利用を検討すべき**。

リスク管理プログラムでは、C-SCRM（サイバーサプライチェーンリスク管理）プログラムのアプローチを採用すべきであり、これにより、ソフトウェア・サプライチェーンリスクの緩和・対応を効率化することができる。NISTが提案する**以下の8つのプラクティスに基づき、ソフトウェアに対するC-SCRMアプローチを確立すべき**である。

1. 組織全体でC-SCRMを統合する。
2. 正式なC-SCRMプログラムを確立する。
3. 重要コンポーネントとサプライヤーを把握し、管理する。
4. 組織のサプライチェーンを把握する。
5. 主要なサプライヤーと緊密に連携する。
6. 主要なサプライヤーをレジリエンス強化及び改善の活動に巻き込む。
7. サプライヤーとの関係を通じて、サプライヤーの評価・監視を行う。
8. ライフサイクル全体の計画を構築する。

また、脆弱なソフトウェアコンポーネントが入り込んでしまった際にそれを緩和するための**脆弱性管理プログラムの採用**、**構成管理**、**ファイアウォールや不正侵入検知/防御システムによる通信管理**、**組織の危機管理計画におけるソフトウェアの考慮**等を実施すべきである。

ソフトウェアベンダーが実施すべき推奨事項

ソフトウェアベンダーは、**通常業務においてソフトウェア開発ライフサイクル（SDLC）を実践することが推奨**される。

また、ベンダーが自社のソフトウェアに関するリスクを緩和するために、**SDLCに対して安全なソフトウェア開発手法を統合する必要**があり、SSDF（セキュアソフトウェア開発フレームワーク）をSDLCに統合することで、悪意あるコンポーネントや脆弱性がソフトウェア・サプライチェーンに入り込むことを防ぐことができる。

ベンダーは、安全なソフトウェア開発を行うために、**以下の準備を行うことが必要**である。

- ソフトウェア開発のセキュリティ要件を定義する。
- SDLCにおけるSSDFの役割と責任を確立する。
- 開発やセキュリティに関するツールチェーンを自動化する。
- ソフトウェアのセキュリティ基準と、セキュリティチェックに必要なデータを収集するためのプロセスを確立する。

また、NISTの推奨事項等を参考に、**開発時にセキュリティに関して緩和策を検討する**ほか、**パッチ適用が可能なソフトウェアの開発、ソフトウェア部品のインベントリ（例：SBOM）の作成・提供を行うべき**である。併せて、**発見された脆弱性に対して可能な限り迅速に緩和策を提供する**ことや、**検出された脆弱性を分析し、その根本原因を特定すること、SDLC全体の改善を図る**ことが必要である。

出所）CISA, “Defending Against Software Supply Chain Attacks” https://www.cisa.gov/publication/software-supply-chain-attacks

【米国】国家のサイバーセキュリティの改善に係る米国大統領令の署名

- 2021年5月12日、バイデン大統領は、連邦政府機関におけるサイバーセキュリティ改善に係る大統領令に署名。
- **官民での脅威情報の共有**、**ソフトウェアサプライチェーンセキュリティ対策**の強化、**ゼロトラストアーキテクチャ**への移行等を通じて、連邦政府機関のサイバーセキュリティ対応能力の向上を図っている。

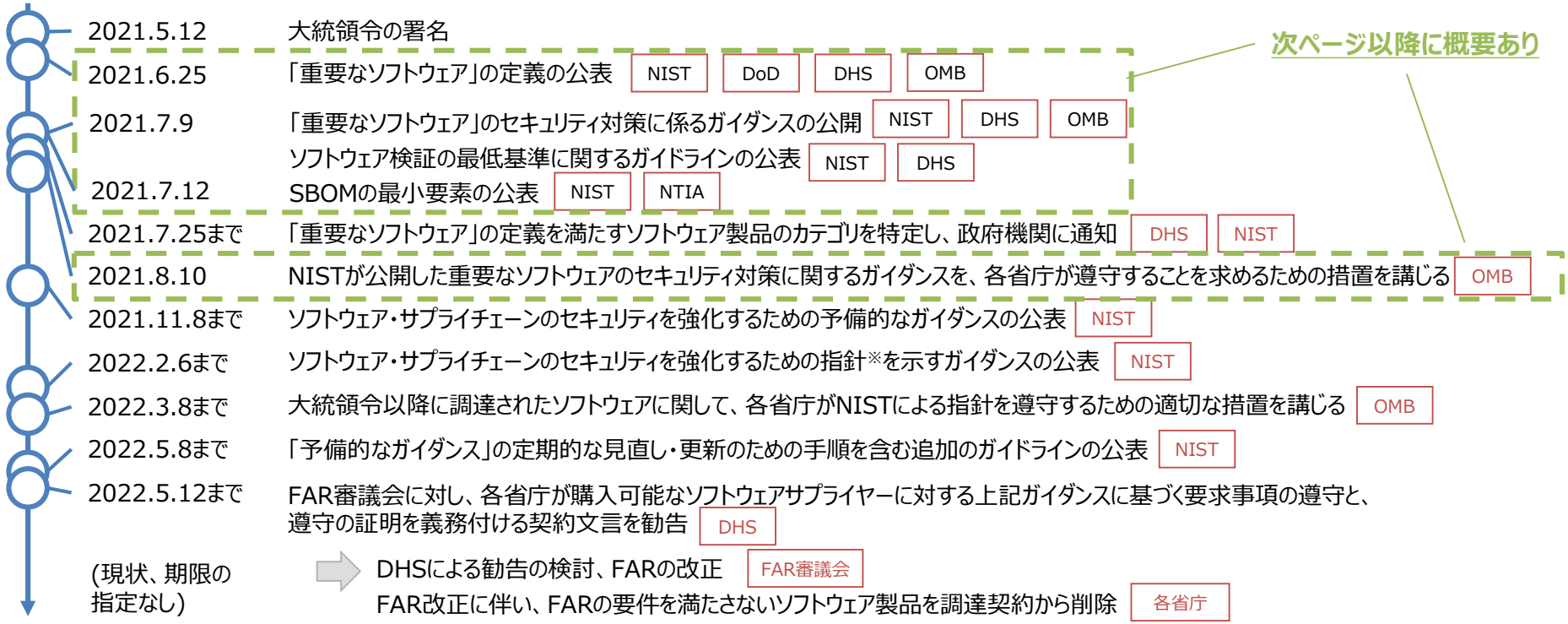
本大統領令における主な指示事項

1 **官民の脅威情報共有における障害の除去** (Section 2)	● ITサービスプロバイダーが連邦政府と確実に脅威情報を共有できるようにした上で、特定のインシデント情報の共有を義務づける。
2 **連邦政府におけるより強力な標準の近代化と導入** (Section 3)	● FedRAMP改定等を通じて、**連邦政府が安全なクラウド及びゼロトラストアーキテクチャに移行することを支援**し、多要素認証と暗号化の導入を義務づける。
3 **ソフトウェア・サプライチェーンのセキュリティ向上** (Section 4)	● NISTを通じて**政府が調達するソフトウェアの開発に関するセキュリティ基準(安全な開発環境の確保や構成要素に関する詳細（SBOM）の開示等を含む)を確立**し、特に**重要なソフトウェアに対して一定の対策を義務づけ**る。 ● 商務省は、既存のラベル表示などを参考にして、消費者向けの情報提供に関するパイロット制度を開始する。
4 **サイバー安全審査委員会の創設** (Section 5)	● 国土安全保障省は、**重大なインシデントが生じた際に政府と民間事業者が共同議長を務める「サイバー安全審査委員会」を設置**し、サイバーセキュリティ向上に向けた具体的な提言を行う権限を与える。
5 **インシデント対応のための標準プレイブックの策定** (Section 6, 7)	● 国土安全保障省は、連邦政府機関によるインシデント対応のためのプレイブックを策定する。 ● 連邦政府機関は、エンドポイント検知・対応(EDR)イニシアチブを展開し、インシデントの検知、積極的なサイバーハンティング、有事対応をサポートする。
6 **調査及び修復能力の向上** (Section 8)	● 連邦政府機関に対してセキュリティイベントログの要件を設け、侵入を検知し、対処する組織能力の向上を支援する。

（出典）各種公開情報より作成

【米国】大統領令におけるソフトウェア・サプライチェーンに関するタイムライン

- 大統領令では、**ソフトウェア・サプライチェーンの確保に向け、NISTが中心となりガイドラインを策定する**旨を指示しており、この**ガイドラインには製品購入者に対するSBOM提供に関する項目も含まれる**。
- また、NISTに対して、NTIAと連携して**SBOMの最小要素を公表すること**を指示している。
- 将来的には、公開されたソフトウェア・サプライチェーンに関するガイダンスの要求事項に基づき、**連邦政府のソフトウェア調達に関するFAR（連邦調達規則）が改正される予定**である。



※ 各製品のSBOMを購入者に提供することに関する標準、手順、基準も含まれる。

出所）White House, “Executive Order on Improving the Nation’s Cybersecurity” https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ , NIST, “Executive Order” https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/executive-order

【米国】「重要なソフトウェア」の定義の公表

- 大統領令を受け、NISTは、**「重要なソフトウェア」の定義に関する文書を6月25日に公開**した。
- 文書では、**5つの属性に基づく「重要なソフトウェア」の定義**に加え、定義に基づき**「重要なソフトウェア」に分類されるソフトウェアカテゴリや具体的な製品種別の暫定リストが明記**されている。
  （正式な製品カテゴリリストはDHS/CISAが策定し、各省庁に通知される予定。）
- **各省庁は、「重要なソフトウェア」への対応を優先的に実施する**ことが大統領令により指示されている。

「重要なソフトウェア (EO-critical software)」の定義※1	該当する製品種別の例※2
いずれかの属性を1つ以上持つコンポーネントを有している、または、直接的にその属性を有しているソフトウェアが「重要なソフトウェア」と定義される。	
権限昇格機能（一時的に管理者権限を得る）の実行や、権限管理に関する機能が設計されている。	ネットワーク管理システム、ネットワーク構成管理ツール、ネットワークトラフィック監視ツール
ネットワークやコンピュータリソースへ直接アクセスするか、アクセスする権限を有する。	Webブラウザ、ルーティングプロトコル、DNSリゾルバやDNSサーバ、SDN制御プロトコル、VPNソフトウェア
データまたはOTへのアクセスを管理するように設計されている。	ID管理システム、バックアップサービスシステム、リカバリーマネージャー、NAS、SAN
ネットワーク制御、エンドポイントセキュリティ等におけるセキュリティ機能のような、信頼性が不可欠な機能を実行する。	OS、ハードディスク暗号化ソフトウェア、パスワードマネージャー、EDR、ファイアウォール、IDS/IPS、
特権アクセスにより、セキュリティ対策が行われている信頼された境界の外で動作する。	SIEM、リモート型脆弱性スキャンツール、パッチ管理ツール、アプリケーション構成管理ツール

※1：適用対象に関して、本番システム用に購入または導入され、運用目的で使用されるすべての形式（スタンドアロンソフトウェア、クラウドベースのソフトウェア等）に適用される。そのため、調査やテストのみに使用されるソフトウェア等、実稼働している本番システムに導入されていないものは適用対象外となる。
※2：複数の属性に該当する製品種別については、代表的な属性においてのみ記載していることに留意。

出所）NIST, “Critical Software”
https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/critical-software

【米国】「重要なソフトウェア」のセキュリティ対策に係るガイダンスの公開

- 大統領令を受け、NISTは、**「重要なソフトウェア」のセキュリティ対策を示すガイダンスを7月9日に公開**した。
- ガイダンスでは、**「重要なソフトウェア」の使用にあたっての5つのセキュリティ対策の目的が定義**され、**それぞれの目的を達成するためのセキュリティ対策が記載**されている。
- OMB（行政管理予算局）は、8月10日に署名した覚書において、**各省庁に「重要なソフトウェア」の特定と、このガイダンスを遵守したセキュリティ対策の実装を要求**。また、**NISTやCISAには、「重要なソフトウェア」の定義、その定義に含まれるソフトウェアカテゴリのリスト、本ガイダンスを必要に応じて更新することを要求**。

「重要なソフトウェア」のセキュリティ対策の目的	セキュリティ対策の例
1 **重要なソフトウェアを実行するためのプラットフォーム※を、不正なアクセスや不正利用から保護する。**	• 重要なソフトウェアのユーザーに対する多要素認証を行う。 • プラットフォームにアクセスする各サービスを一意に識別、認証する。 • ネットワーク分離やプロキシの利用等によりネットワークを保護する。
2 **重要なソフトウェアを実行するためのプラットフォームで使用されるデータの機密性、完全性、可用性を保護する。**	• データに対するアクセス管理を実施する。 • 機密データを、NISTの暗号化標準に準拠して暗号化する。 • データ通信を暗号化することで、転送中のデータを保護する。
3 **重要なソフトウェアを実行するためのプラットフォームと、それらのプラットフォームに展開されているすべてのソフトウェアを特定して管理し、重要なソフトウェアが悪用されることから保護する。**	• プラットフォーム上のすべてのソフトウェアを特定し、資産管理、パッチ管理、構成管理を行う。
4 **重要なソフトウェアや、当該ソフトウェアを実行するためのプラットフォームに関連する脆弱性やインシデントを早急に検出、対応、回復する。**	• プラットフォーム上のソフトウェアのセキュリティイベントを監視する。 • エンドポイントにおけるセキュリティ対策を行う。 • プラットフォーム間のネットワークトラフィックを監視する。
5 **重要なソフトウェアや、当該ソフトウェアを実行するためのプラットフォームに関するユーザー及び管理者のセキュリティの理解を促進する。**	• すべてのユーザー及び管理者に対するセキュリティトレーニングを行う。 • トレーニングの効果を強化するための活動を行う。

※ エンドポイントの端末、サーバー、クラウドサービスのリソース等の「重要なソフトウェア」が動作するプラットフォームを意味する。

出所）NIST, “Security Measures for “EO-Critical Software” Use”
https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/security-measures-eo-critical-software-use-2

【米国】SBOMの「最小要素」の定義

- 大統領令を受け、NTIAは当該定義に関するパブリックコメントを実施。**ソフトウェア関連の企業や専門家からの意見を踏まえ、SBOMの「最小要素」の定義を7月12日に公開**した。
- SBOMの「最小要素」には、**「データフィールド」、「自動化サポート」、「プラクティスとプロセス」**の3つのカテゴリが含まれ、**コンポーネントを一覧化した部品表に含まれる情報だけでなく、SBOMの利活用者が実施すべき事項**も規定されている。
- 定義された「最小要素」に基づき、**ソフトウェア購入者へのSBOM提供に関するガイダンスが整備**されるほか、将来的には、**各省庁のソフトウェアに関する取組が本定義に基づき実施される**ことが明記されている。

3つのカテゴリ	「最小要素」の概要	「最小要素」の具体的な定義
データフィールド（Data Fields）	**各コンポーネントに関する基本情報を明確化すること**	以下の情報をSBOMに含めること。 • サプライヤー名 • コンポーネント名 • コンポーネントのバージョン • その他の一意な識別子 • 依存関係 • SBOMの作成者 • タイムスタンプ
自動化サポート（Automation Support）	**SBOMの自動生成や可読性などの自動化をサポートすること**	SBOMデータは機械判読可能かつ相互運用可能なフォーマットを用いて作成され、共有されること。現状では、国際的な議論を通じて策定された、SPDX、CycloneDX、SWIDタグを用いること。
プラクティスとプロセス（Practices and Processes）	**SBOMの要求、生成、利用に関する運用方法を定義すること**	SBOMを利活用する組織は、以下の項目に関する運用方法を定めること。 • SBOMの作成頻度 • SBOMの深さ • 既知の未知 • SBOMの共有 • アクセス管理 • 誤りの許容

出所）NTIA, “The Minimum Elements For a Software Bill of Materials (SBOM)”
https://www.ntia.doc.gov/report/2021/minimum-elements-software-bill-materials-sbom

【米国】ソフトウェア検証の最低基準に関するガイドラインの公表

- 大統領令を受け、NISTは、**ソフトウェア検証の最低基準に関するガイドラインを7月9日に公開**した。
- ガイドラインでは、**ベンダーや開発者によるソフトウェア検証の際に推奨される、11の最低基準**が示されている。
- 最低基準は、実行可能なコンピュータプログラムすべてに推奨され、**将来的には、ソフトウェアベンダーや開発者に対する強制基準の基礎となりうる**ことが明記されている。

ソフトウェア検証において推奨される11の最低基準

1. 脅威分析

ソフトウェア開発の早期に脅威分析を実施し、設計段階でのセキュリティ問題を特定する。

2. 自動化ツールの使用

静的解析及び動的解析の一部の検証において、自動化ツールを活用する。

3. ソースコードに対する静的解析

静的解析ツールを使用してソースコードの解析を行い、様々な種類の脆弱性を検出する。解析は、ソースコード作成直後に行う。

4. ハードコードされたクレデンシャル情報の確認

ハードコードされたパスワードや暗号鍵等がないかを確認するために、静的解析ツールや手動レビューにより確認する。

5. チェック機能・保護機能を用いたプログラム実行

開発中や完成後のソフトウェアに対して、プログラム言語のビルトインチェック機能や保護機能を用いてプログラムを実行する。

6. ブラックボックステスト

セキュリティで重要とされている範囲を包括的にカバーしたテストケースに基づき、ブラックボックステストを実施する。

7. コードベーステスト（ホワイトボックステスト）

ソースコードの仕様に基づいたホワイトボックステストを行う。ほとんどのコードに対して、単体テストの時点で実行する必要がある。

8. 回帰テスト

以前にテストしたソフトウェアが、変更後もまだ動作するかどうかを、再度実行して確認する。

9. ファジングテスト

入力値を自動で大量生成するツール（ファザー）を使用して、ファジングテストを実行する。

10. Webアプリケーションのスキャン

ソフトウェアがWebサービスを提供する場合は、Webアプリケーションをスキャンする動的解析ツールやIASTツール※を使用して脆弱性を検出する。

11. コンポーネントの監視

ソフトウェアに含まれているコンポーネント（OSS等の外部ソース含む）は、脆弱性データベース等を活用して、その脆弱性を継続的に監視する必要がある。

- 脅威分析に関する基準
- 静的解析に関する基準
- 静的解析・動的解析の両方に関する基準
- 動的解析に関する基準
- コンポーネントの脆弱性に関する基準

※：Interactive Application Security Testingの略で、実際に動作しているアプリケーションのデータフローを解析し、脆弱性の検出を行うテスト手法のこと。

出所）NIST, “Recommended Minimum Standards for Vendor or Developer Verification (Testing) of Software Under Executive Order (EO) 14028
https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/recommended-minimum-standards-vendor-or

【米国】NTIA Software Component Transparency ～ NTIA WGの今後の課題領域 ～

- 2021年4月29日に開催されたNTIA Software Component Transparencyの会合において、同取組の今後の課題領域が特定された。

NTIA Software Component Transparencyの会合（4/29）で認識された今後の課題領域		今後の課題領域が割り当てられているワーキンググループ
定義と改善 Defining and Refining	• SBOMに求められる最低限の情報の整理 • ソフトウェアの脆弱性と悪用可能性に関する管理方法の整理（VEX） • SBOMに関する共通言語の整理	**■Framing WG** SBOMの仕様を定義し、改善することに焦点を置く
ツール Tooling	• ソフトウェア識別ツールの調査 (SPDX、SWID、CycloneDX) • SBOMサプライヤーに向けたSBOM解説書の作成	**■Formats and Tooling WG** SBOMの作成と使用を自動化する方法に焦点を置く
デモンストレーション Demonstrations	• 医療機器メーカー（MDM）に向けたSBOM活用のガイドラインの作成 • その他分野（自動車、エネルギー）への拡張	**■Healthcare Proof of Concept WG** ヘルスケア分野でのSBOM活用に関するPoCを実施する
ビジネスプロセス Business Processes	• SBOMサプライヤーへのヒアリング • SBOMを導入する際の手引きの策定	**■Automotive Proof of Concept WG** 自動車分野でのSBOM活用に関するPoCを実施する ※ 2021年に新たに設立
認知/採用 Awareness/Adoption	• FAQの拡充（コストと投資に関するQA） • SBOM促進に向けた機会の創出 （ウェビナー、ポッドキャスト、RSAカンファレンスへの参加等）	**■Awareness and Adoption WG** SBOMの認知と導入、導入促進に焦点を置く

出所）NTIA公開資料に基づき整理

【米国】NTIA Software Component Transparency ～ ヘルスケア分野のPoCにおいて確認されたSBOM活用のユースケース ～

- **NTIAが、医療機器メーカーと医療機関の両方を巻き込んで2018年7月から開始**したヘルスケア分野でのSBOM PoCでは、医療機器の調達管理、資産管理、リスク管理、脆弱性管理、及び法務管理に関するユースケースに関して、SBOM活用によるメリットや効果が確認された。

5つのSBOM活用ユースケースにおけるヘルスケア分野PoCでの実施項目

調達管理

医療機器調達・導入の際、SBOMを活用することで、**事前にリスク・脆弱性を把握**し対応することを可能にする

- 脆弱性情報データベースとリンクさせ、自動的に医療機器の脆弱性情報を取得する
- 機器導入時に、ソフトウェアのサポート年数等に関する情報を提供する

資産管理

医療機器導入後、SBOM活用による長期的・定期的な情報更新により**医療機器の入れ替えの意志決定を支援**

- 医療機器のリスクアセスメントの標準化を推進する
- ソフトウェアのサポート期限等の情報を随時更新する
- 棚卸資産台帳の構築を支援する

リスク管理

SBOMに基づき、調達時および継続的に悪用可能性（≠脆弱性）を特定することで、**リスクレベルの把握・低減を支援**

- 新規機器のネットワーク接続時のリスク評価を行う
- それぞれの脆弱性に関するリスクレベル評価を行う
- 新しい脆弱性発見時、医療機関内のリスク再検証を支援する

脆弱性管理

SBOMを活用することで、**脆弱性の把握及び管理を継続的に支援**

- リスク管理の過程で脆弱性情報を自動的・継続的に入手・脆弱性管理に活用する
- 通常の脆弱性スキャンをSBOMによる情報提供で補完する

（Phase 2で新たに追加）

法務管理

SBOMに基づき、法的な**契約書類においてサイバーセキュリティ上のセーフガードを規定**する

出所）ヘルスケア分野におけるSBOM PoCに関するNTIA公開資料に基づき整理

【米国】NTIA Software Component Transparency ～ ヘルスケア分野のPoCにおいて確認されたSBOM活用の課題 ～

- ヘルスケア分野でのPoCでは、フェーズ1において、ツールによる自動化に関する課題や統一的なフォーマットに関する課題が抽出された。
- フェーズ2では、当該課題に対して関係するWGと連携しながら検討が進められている。

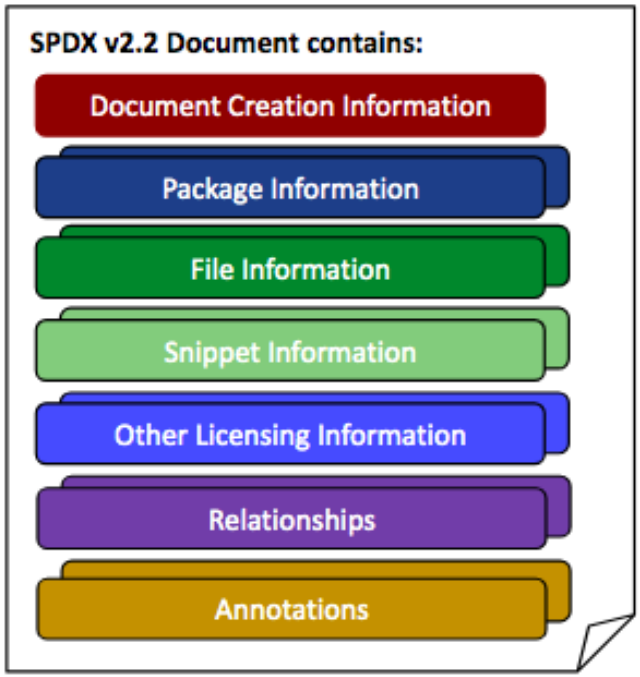
Phase 1 : 2018年7月～2019年10月	Phase 2: 2019年10月～
<u>ツールによる自動化に関する課題</u> • 医療機器メーカーごとにSBOMを作成した結果、作成過程での普遍的なツールの利用等について統一的な検討はできていない • 一部手動で入手する必要のある情報（仕様書PDF内に含まれた情報など）があったが、利便性の高い自動化ツールが存在しない	ソフトウェアベンダーと共同で自動化ツールの開発を検討中 （SBOM作成・配布及び医療機関での統合的利用）
<u>統一的なフォーマットに関する課題</u> • 一部の資産管理手法と統合的に利用することが困難 （フォーマットを統合できていない） • SBOMコンポーネントに関する名前付けが標準化されていない	SPDX、CycloneDXのサポートを検討 統一的な名前付け基準の策定
• SBOMの属性に関する**<u>URIが標準化されていない</u>** • 手動で対応させる必要があり、主観的となる	purl、CPEを活用した識別子を検討
• SBOMの**<u>情報の正確性・完全性を監査・検証するプロセスがない</u>** （現状はSBOMの情報は無条件に受け入れられている）	

出所）ヘルスケア分野におけるSBOM PoCに関するNTIA公開資料に基づき整理

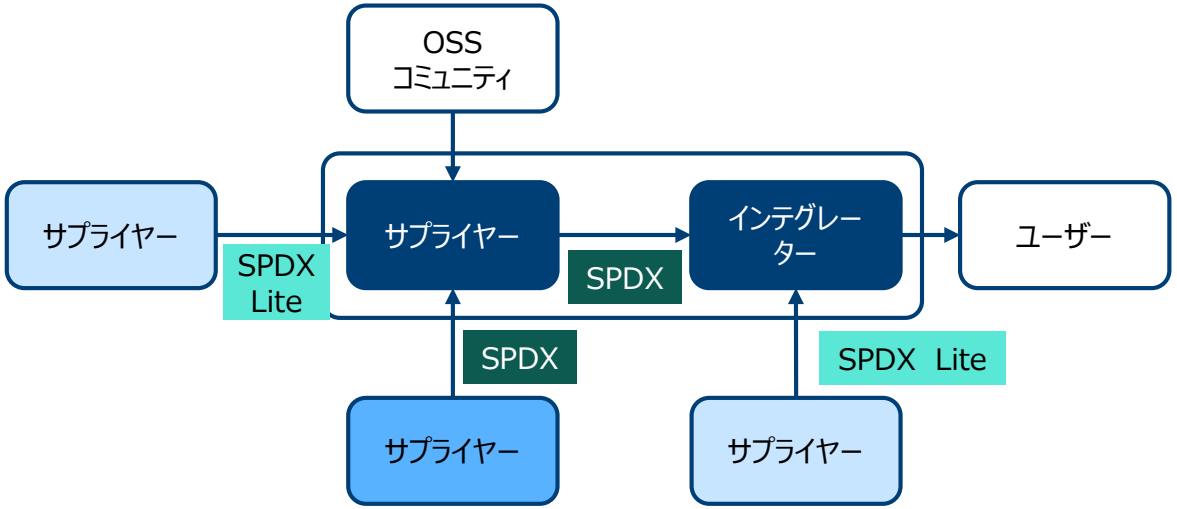
SPDX仕様の国際標準化（ISO/IEC 5962:2021）

- 2021年8月、SBOM情報を伝達するための仕様である**SPDX (Software Package Data Exchange)が、ISO/IEC 5962:2021として国際標準化**された。
- SPDXは、Linux Foundationが支援するSPDX Working Groupによって策定され、Intel、Microsoft、Siemens、ソニー、Synopsys、VMWare、Wind River等の企業において既に活用されている。
- OpenChain Japan WGで議論されたSPDX Liteも、国際標準の一部として含まれている。

SPDXファイルの構成要素



SPDX･SPDX Liteを用いたSBOM情報伝達のイメージ



出所）Linux Foundation, “Software Package Data Exchange (SPDX®) Specification Version 2.2” https://spdx.dev/wp-content/uploads/sites/41/2020/08/SPDX-specification-2-2.pdf
OpenChain project Japan workgroup, “SPDX Lite” https://wiki.linuxfoundation.org/_media/openchain/spdx-lite-overview-20190905.pdf

1. サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）とその実装へ向けた取組の方向性

2. 最近のインシデント事例

3. ソフトウェア管理等に関する諸外国の取組状況

4. 本タスクフォースにおける検討事項

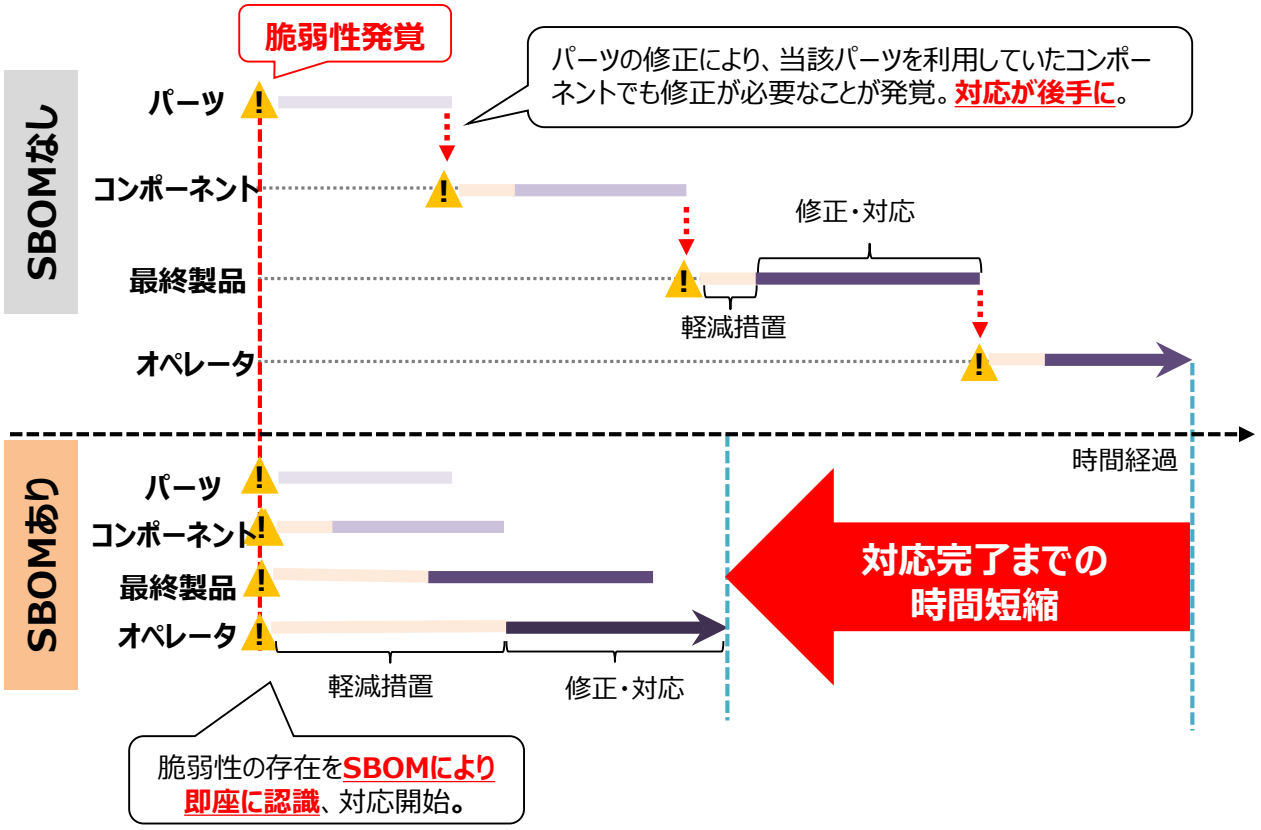
（１）国内でのSBOM活用促進に向けた実証

（２）OSS管理手法に関する事例集の拡充

SBOMに係る取組の進展

- 米国NTIAが2018年から主導するSoftware Component Transparencyでは、ヘルスケア分野における実証事業（PoC）に続いて、自動車分野・電力分野にも取組が拡大。
- 米国では、2021年5月に発令された大統領令においてもSBOM提供について言及されており、今後、政府調達要件として整備が進むものと想定。
- 米国の動向も踏まえ、日本においても、業界構造や商習慣を考慮しつつSBOMの導入効果やコスト等を明らかにすべく、SBOM活用に向けた実証事業を実施。

SBOMの導入効果：脆弱性発覚から復旧までの時間を短縮



米国NTIAにおけるSBOMのPoC

ヘルスケア分野（病院、医療機器）

病院、医療機器メーカー、ベンダーが参加。2回のPoCを経てSBOM活用の手法、課題等を公開。4/29のNITA会合にて、医療機器メーカーにおけるSBOM活用に向けたガイドラインを取りまとめる予定と発表。

自動車産業分野

Auto-ISACを中心としたサプライヤー中心のプロジェクト。ヘルスケア分野のPoCを参考にしつつ、自動車産業分野でのSBOMの普及促進を目的として、SBOM構築方法や得られた教訓・課題等を確認する。12ヶ月ほどかけてサプライヤー向けの推奨事項がとりまとめられる予定。

電力分野

INL主導で、電力会社、電力機器ベンダー、ソフトウェアベンダー、電気協会等が参加。米国エネルギー省からもプレゼンターとして参加。2021年中のPoC実施完了に向け、目的、実施内容、スケジュールに関する議論を経て、9/1からPoCを実施中。

SBOM導入・活用の障害・課題に関する整理

- SBOM活用による効果が想定される一方で、**SBOM導入にかかるコスト等が障壁となり、日本全体としてSBOMの導入・活用が進んでいない**。
- 本実証事業においては、どのようにSBOMを活用すれば、**SBOM導入によって得られる効果が大きくなり、普及に繋がるかを確認したい**。

SBOM導入・活用の障害・課題

● SBOM導入にかかるコスト

– SBOMの導入・管理にかかるコストが新たに発生。

– 効果に対してどの程度のコストをかけるべきか判断に必要な情報が少ない。

– 多数のSBOMを手動で管理するとコストが膨大になるためツールによる自動化が考えられるが、下記のような課題が存在。

- ツールの導入コスト・ランニングコストが発生。
- ソフトウェアIDやSBOM形式が統一されていないなど、自動化の障害が存在。

● SBOM情報開示に対するサプライヤーの抵抗感

– サプライヤーによるSBOM生成・情報開示に関する抵抗感が強い。

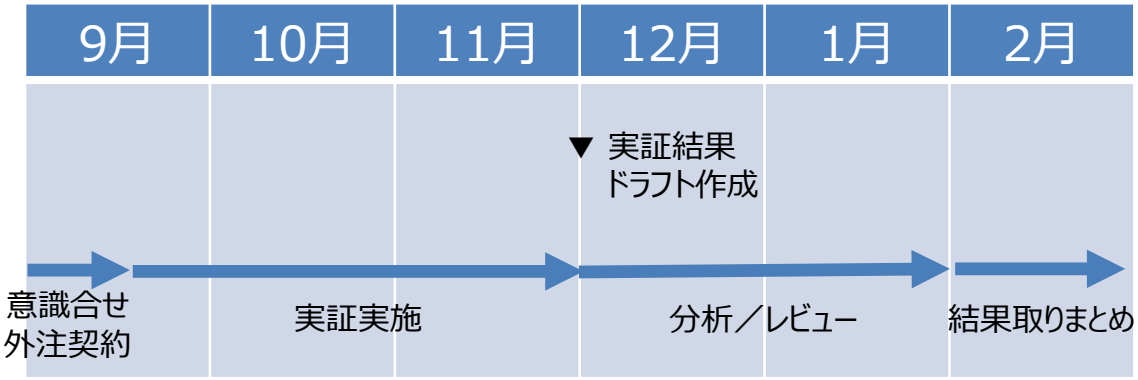
SBOM実証の対象ソフトウェア・体制・スケジュール

- ユーザー企業や製品ベンダーからのご協力が見込まれることから、**自動運転システム検証基盤ソフトウェア「GARDEN」を実証の対象ソフトウェアに選定**。

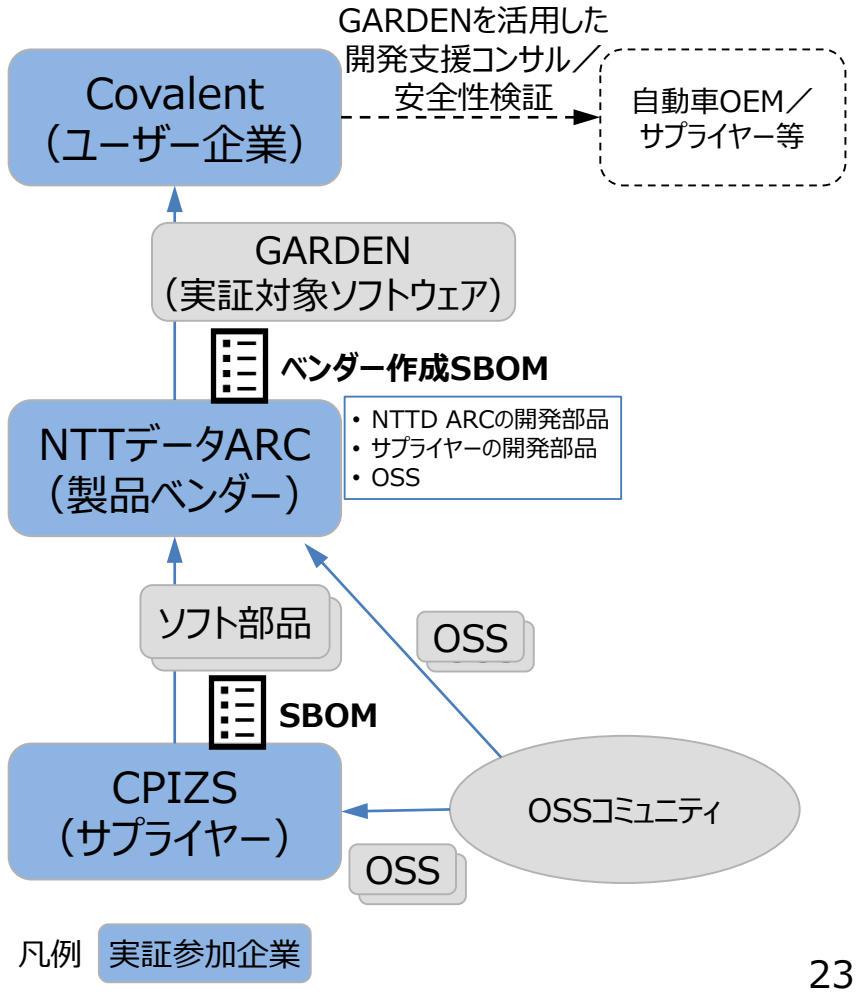
実証対象ソフトウェア 「GARDEN」

名称	GARDEN Scenario Platform
製品ベンダー	株式会社NTTデータ オートモビリジェンス研究所（NTTデータARC）
概要	• 自動運転システム開発向け検証基盤ソフトウェア。 • 自動運転ソフトウェアの安全性評価のための機能動作シミュレーションのシナリオ生成機能を提供。 ➢ モデリング、走行データ分類、軌跡抽出道路編集、シナリオ組合せテスト、シナリオ実行 • オープンソースとして、ソースコードを公開。

想定スケジュール



実証体制（GARDENのサプライチェーン）



SBOM実証の内容（案）

- 実証においては、作成手段や作成者等の条件を設定して、SBOMの実際の効果やコストを比較し、今後の検討事項を整理。

比較項目

- **SBOMの効果**
  - 脆弱性管理　　脆弱性特定工数、脆弱性修正までの期間、脆弱性残留リスク等の低減
  - ライセンス管理　　ライセンス特定工数、ライセンス違反残留リスク等の低減
- **SBOMのコスト**
  - 初期コスト　　体制構築、環境整備
  - SBOM作成コスト　　作成工数、作成ツール費用
  - SBOM活用コスト　　部品管理工数（脆弱性の影響特定など）、管理ツール費用

比較条件

- そもそもソフトウェアの部品管理を行わない場合
- SBOMという形ではないが、何らか部品管理を実施する場合
- SBOMをユーザーが作成する場合
- SBOMをベンダーが作成する場合（手動で行う場合、ツールを利用する場合）

- **実証を通じてSBOMの実際の効果やコストを算出。**
- **国外の取組の進展も踏まえ、SBOMの効果的な活用方法を検討、今後の検討事項を整理。**

SBOMに関する施策の進め方（案）

- 国内施策および国際連携により、SBOMに係る対応を進める。
- 令和3年度の実証を通じてSBOMの効果的な活用方法を検討（STEP1）。
- STEP1の結果を踏まえて令和4年度以降、実証の対象を拡大し必要な制度、ツール整備を図る。

＜施策テーマ＞

	施策テーマ	施策
国内施策	(1) 国内産業のSBOM対応促進	**① 国内産業のSBOM普及啓発** • 実証やガイダンス等により国内産業へのSBOM普及促進を図る。
		②SBOM普及に向けた論点整理 ①で明らかにした論点を整理し、必要な制度・ツール等を整備する。 例：費用負担やリスク負担、知財権保護等の整理。自動化に向けたツール環境やソフトウェアID等の整備。
国際連携	(2) 日米の協力関係構築	**③SBOM検討に係る日米協力** OSS事例集や国内実証のコスト評価結果などを提供することにより、日米検討の協力関係を構築し、ツール等の整備における必要な調整を図る。

＜検討のステップ＞

STEP1：【R3年度実施】

実証を通じたSBOMの効果的な活用方法の検討

STEP2：【R4年度実施】

実証の対象拡大による課題整理（サプライチェーンにおける共有等）

STEP3：【R4年度～】

制度、ツールの検討・整備
国外との制度調和

1. サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）とその実装へ向けた取組の方向性

2. 最近のインシデント事例

3. ソフトウェア管理等に関する諸外国の取組状況

4. 本タスクフォースにおける検討事項

（１）国内でのSBOM活用促進に向けた実証

（２）OSS管理手法に関する事例集の拡充

OSS管理手法に関する事例集の拡充

- **「OSSの利活用及びセキュリティ確保に向けた管理手法」をまとめた事例集を作成し、2021年4月21日に公開**。参考となる事例を共有して企業における適切なOSS利用を促進。日本から働きかけることで日米でOSSの活用・管理に関するベストプラクティスを共有する機会の確保を目指す。
- 令和3年度も、事例の拡充に向けてヒアリングおよび机上調査を継続。

https://www.meti.go.jp/press/2021/04/20210421001/20210421001.html