経済産業省

資料 3

最近の産業サイバーセキュリティに関する動向について

令和3年11月

経済産業省　商務情報政策局

サイバーセキュリティ課

１．はじめに
～サイバー攻撃の脅威レベルの向上

２．サイバーセキュリティに関する諸外国の検討状況

３．産業分野でのサイバーセキュリティ対策強化に向けた取組

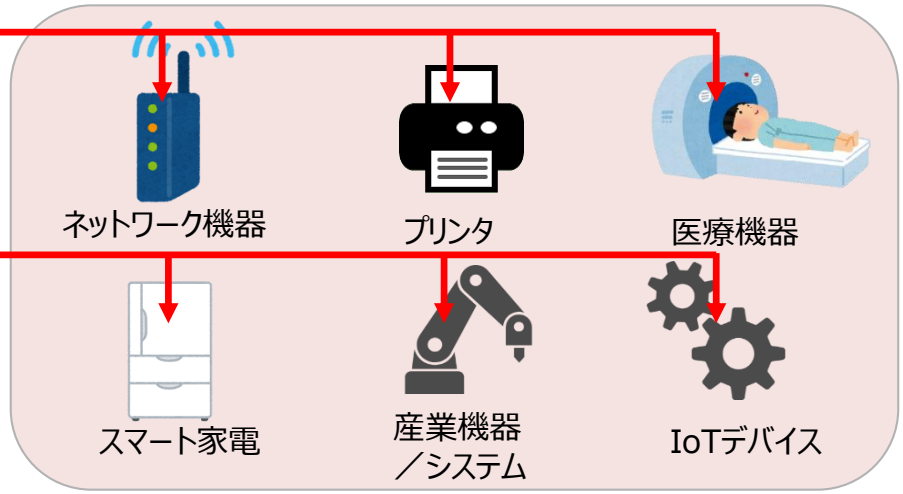
プロトコルスタックの脆弱性：“Ripple20”

- 2020年6月、JSOF社は、**Treck社※1が開発したTCP/IPプロトコルスタック※2「Treck TCP/IP Stack」に複数の脆弱性**があることを発表（発表年や当スタックが20年以上前から存在していること等に由来し、19の脆弱性の総称をRipple20と命名）。遠隔の第三者によって、**任意のコード実行、情報の窃取、サービス運用妨害（DoS）等の攻撃を受ける可能性**があり、最新バージョンへの更新やパッチの適用、 IPパケットのフィルタリング等の対策を呼び掛けている。
- Treck TCP/IP Stackは多数の企業が製品に採用しており、数億台かそれ以上の機器が影響を受けるとされ、家庭向けデバイス、ネットワーク機器、医療機器、産業制御機器／システム、重要インフラ分野などの幅広い領域への影響が懸念される。

◆攻撃イメージ／影響範囲の例

想定被害：任意のコード実行、情報漏えい、DoS

Treck TCP/IP Stackの採用製品は、下図以外にも多岐に渡る



- ✓ Treck TCP/IP StackはHP社、Schneider Electric社、Intel社、Rockwell Automation社、Caterpillar社、Baxter社等の製品が採用。
- ✓ 同様の脆弱性が、関連する他のTCP/IPスタックにも存在することが報告されている。

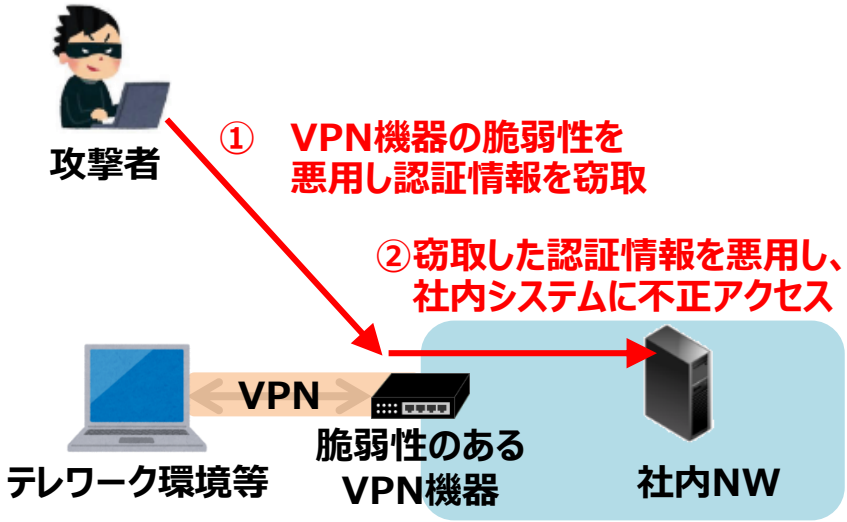
https://www.jsof-tech.com/ripple20/

※1　組み込み機器向けのインターネットプロトコルスタックを設計・開発する米国の企業
※2　階層構造で構成されるインターネットプロトコル群

VPN機器の認証情報流出

- **VPN機器の脆弱性**が相次いで報告され、そうした脆弱性を**悪用するコードが公開**されるなど深刻な状況が発生。**攻撃者はこうした脆弱性を通じて直接的に社内ネットワークへ侵入**し、攻撃を展開。
- 2020年8月、Pulse Secure製VPN機器の脆弱性が悪用され、**国内外900以上の事業者からVPNの認証情報が流出**。2020年11月、Fortinet製品の**VPN機能の脆弱性の影響を受ける約5万台の機器に関する情報が公開**。**認証情報等が悪用されることで容易に侵入されるおそれ**。
- **どちらのケースも既に悪用されている可能性**があるため、**機器のアップデートや多要素認証の導入といった事前対策**に加え、事後的措置として**侵害有無の確認や、パスワード変更等の対応**が必要。

VPN機器に対する不正アクセス



Pulse Secure製VPN機器の脆弱性

2019年4月	脆弱性情報公開
2019年8月	脆弱性の悪用を狙ったとみられるスキャンを確認
2019年9月	脆弱性を悪用したとみられる攻撃を確認
2020年8月	国内外900社（国内は38社）の認証情報が公開

Fortinet製FortiOSの脆弱性

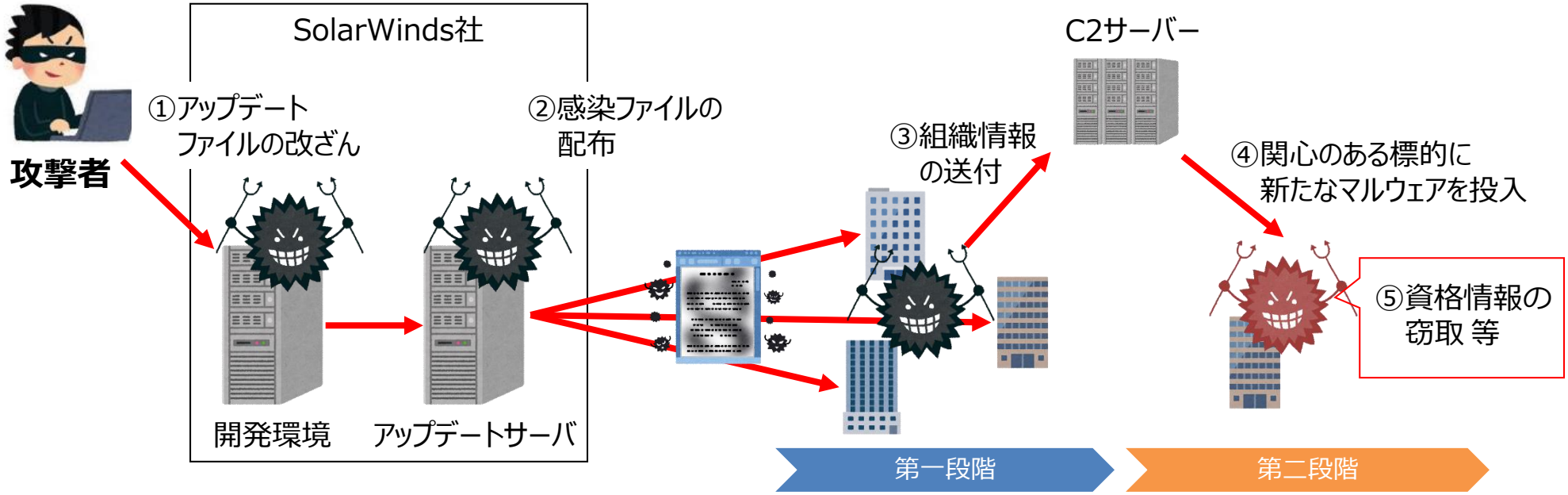
2019年5月	脆弱性情報公開
2019年8月頃	脆弱性の詳細情報公開、悪用やスキャン開始
2020年11月	脆弱性の影響を受ける約5万台の機器情報が公開 IPアドレス、ユーザーアカウント名、平文パスワード等

https://www.jpcert.or.jp/newsflash/2020112701.html
https://www.jpcert.or.jp/at/2019/at190033.html

SolarWinds Orion Platformのアップデートを悪用した攻撃

- 2020年12月13日、SolarWinds社は同社のネットワーク監視ソフトウェア「Orion Platform」に、**正規のアップデートを通じてマルウェアが仕込まれた**ことを公表。
- 攻撃は2019年9月には始まっていたとみられ、2020年3月～6月のアップデートファイルが侵害されたことで、米政府機関等を含む**最大約18,000組織が影響**を受けたとされる。
- 初期段階のマルウェアは、セキュリティサービスの検知を回避しつつ被害組織の情報をC2サーバーへ送信。**攻撃者が関心のある標的に対しては第２段階のマルウェアが投入**され、資格情報を窃取した上で、**米国政府内、政府間のやり取りを傍受していた可能性が指摘されている。**

◆攻撃イメージ



（出典）各種公開情報に基づき経済産業省作成

１．はじめに
　～サイバー攻撃の脅威レベルの向上

２．サイバーセキュリティに関する諸外国の検討状況

３．産業分野でのサイバーセキュリティ対策強化に向けた取組

【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】「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。
- 今後、本定義を踏まえた**ソフトウェア・サプライチェーンのセキュリティ強化に関するガイダンスが策定**される。

「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】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】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・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

【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

１．はじめに
　～サイバー攻撃の脅威レベルの向上

２．サイバーセキュリティに関する諸外国の検討状況

３．産業分野でのサイバーセキュリティ対策強化に向けた取組

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）の策定

- 2019年6月、産業・社会の変化に伴うサイバー攻撃の脅威の増大に対し、リスク源を適切に捉え、検討すべきセキュリティ対策を漏れなく提示するため、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）を策定し、新たなモデル（**三層構造**と**６つの構成要素**）を提示。

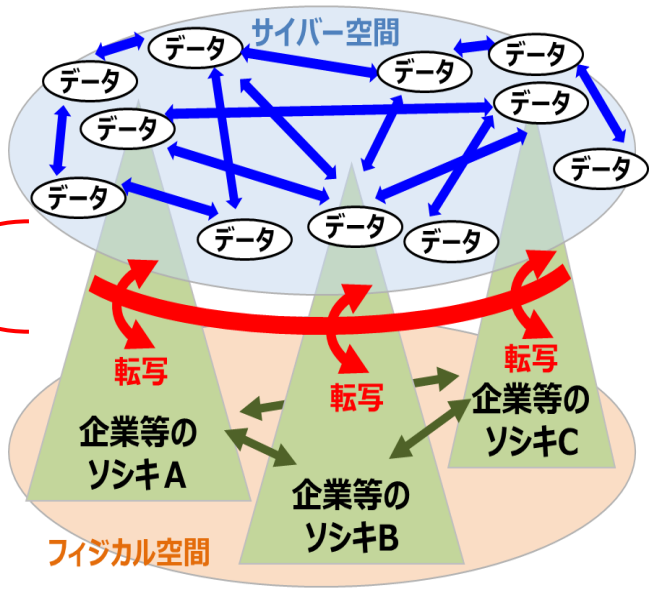
三層構造

「Society5.0」における**産業社会を３つの層に整理**し、セキュリティ確保のための信頼性の基点を明確化

サイバー空間におけるつながり
【第３層】
自由に流通し、加工・創造されるサービスを創造するための**データの信頼性**を確保

フィジカル空間とサイバー空間のつながり
【第２層】
フィジカル・サイバー間を正確に**“転写”する機能の信頼性**を確保
（現実をデータに転換するセンサーや電子信号を物理運動に転換するコントローラ等の信頼）

企業間のつながり
【第１層】
適切な**マネジメントを基盤に各主体の信頼性**を確保



６つの構成要素

対策を講じるための単位として、**サプライチェーンを構成する要素を６つに整理**

構成要素	定義
ソシキ	• バリュークリエイションプロセスに参加する企業・団体・組織
ヒト	• ソシキに属する人、及びバリュークリエイションプロセスに直接参加する人
モノ	• ハードウェア、ソフトウェア及びそれらの部品 操作する機器を含む
データ	• フィジカル空間にて収集された情報及び共有・分析・シミュレーションを通じて加工された情報
プロシージャ	• 定義された目的を達成するための一連の活動の手続き
システム	• 目的を実現するためにモノで構成される仕組み・インフラ

第3層TF：サイバー空間における価値創造を支えるデータマネジメントの枠組みの策定

- データマネジメントに関する定義を明確化し、フレームを設定することで、主体間を転々流通するデータに関する**リスクポイントの洗い出しを可能に**する。
- また、本枠組みを**共通の定規として利用**することで、各国・地域などの**主体間のデータに関するルールのギャップ/データの流通プロトコルの問題を可視化、データの囲い込みを回避する**取組につなげる。
- 「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）」の**骨子案を取り纏め、パブリックコメントを実施**。（2021/7/15～10/11）

https://www.meti.go.jp/press/2021/07/20210715005/20210715005.html

データマネジメントの新たな捉え方

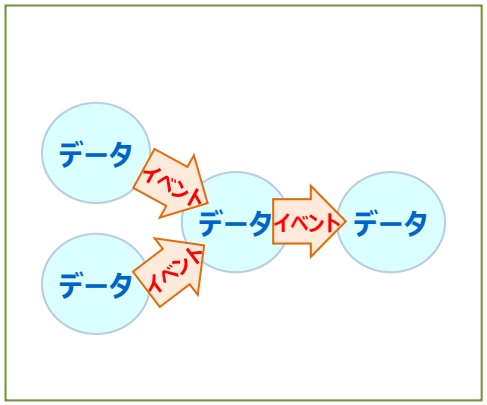
▶「データの "**属性**" が "**場**" における "**イベント**" により変化する過程をライフサイクル全体にわたって管理すること」

属性		場		イベント
データが有する性質	✖	特定の規範を共有する範囲	✖	データの属性を生成・変化させる処理

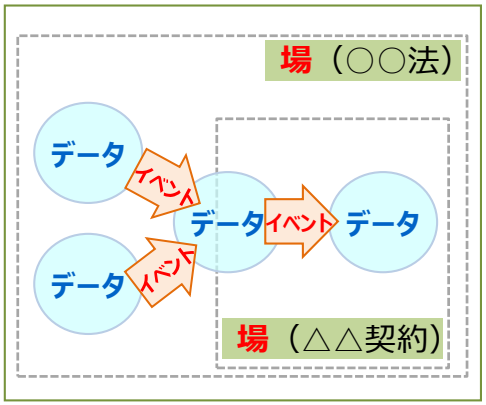
新たな捉え方への当てはめステップ

▶4つのステップに沿ってバリュークリエイションプロセスにおけるデータの状態を可視化しリスクを洗い出す。

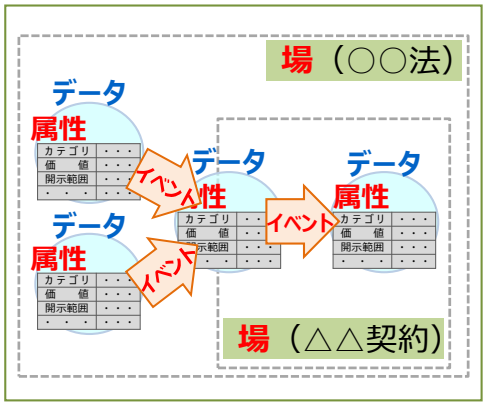
STEP 1
データ処理フロー（「イベント」）の可視化



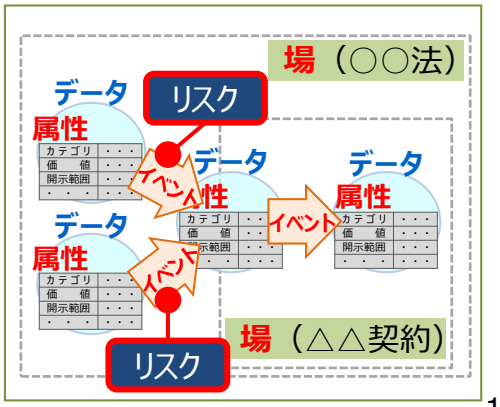
STEP 2
必要な制度的保護措置（「場」）の整理



STEP 3
「属性」の具体化



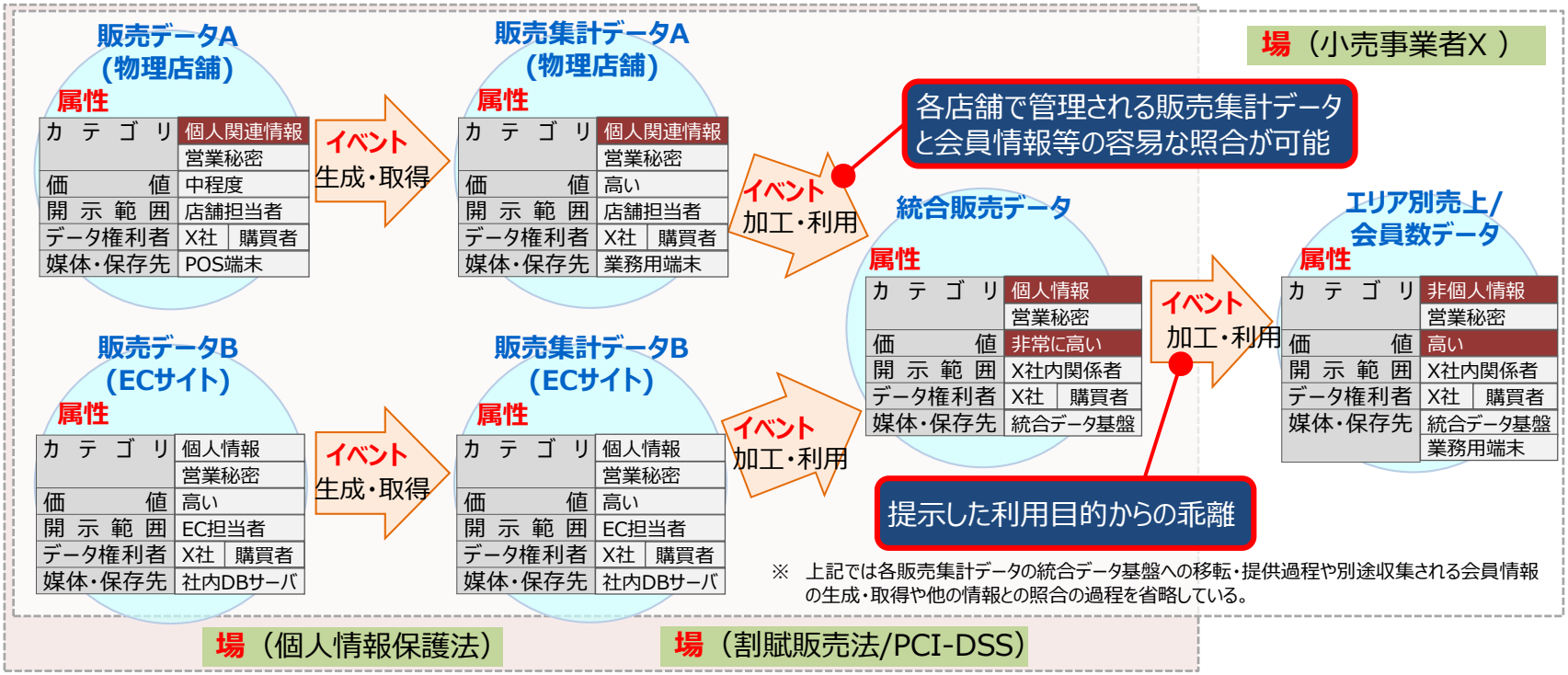
STEP 4
「イベント」ごとのリスクの洗い出し



第3層TF：フレームワークのユースケースに係る検討（POSデータ活用事例）

- ユースケースのひとつとして、小売業におけるPOSデータの活用事例にフレームワークを適用。
- 販売データの生成・取得からマーケティング目的での加工・利用に至るまでの一連の利活用プロセスを可視化するとともに、今後のセキュリティ水準等の向上のために必要なアクションを明確化。

新たな捉え方の適用（小売業におけるPOSデータの活用事例）



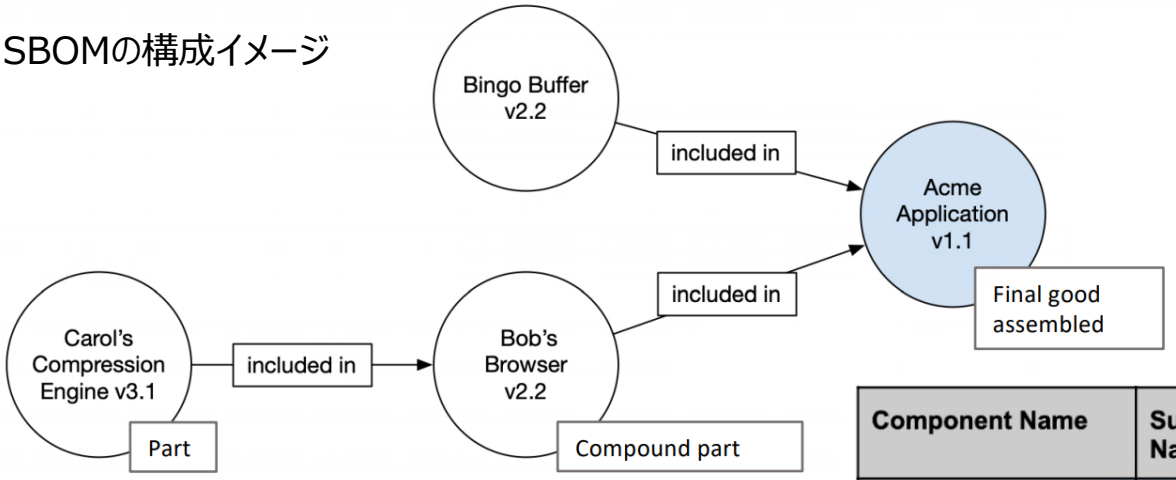
新たな捉え方の適用を通じてx社が導き得るアクション（例）

- 一律のデータ保護水準を確保することが難しい各物理店舗において、他データとの照合等を通じて個人情報に該当するデータが保有されないことを改めて確実なものとすべく、統合データ基盤で管理される会員情報に対する各店舗、支社によるアクセス状況のレビュー、アクセス制御ポリシーその他の運用規定の見直し等を行う
- 購買者に関するデータの利用実態を踏まえ、自社の個人情報保護方針や会員規約等の一部（利用目的に関する条項等）を改定する

ソフトウェアTF： SBOMについて

- SBOM （Software Bill of Materials）とは、ソフトウェアの部品構成表のこと。ソフトウェアを構成する各コンポーネントを誰が作り、何が含まれ、どのような構成となっているか、等を示す。
- SBOMによりソフトウェアの構成情報を詳細に把握することができ、ライセンス管理や脆弱性対応への活用が期待できる一方、その作成や管理、サプライチェーンにおける共有等において課題が存在。
- 米国NTIA（電気通信情報局）では、 2018年に「Software Component Transparency」に関するMultistakeholder Meetingを設置し、ヘルスケア分野におけるPoC等を実施するなど、SBOMの構成や活用について議論を重ねている。

SBOMの構成イメージ



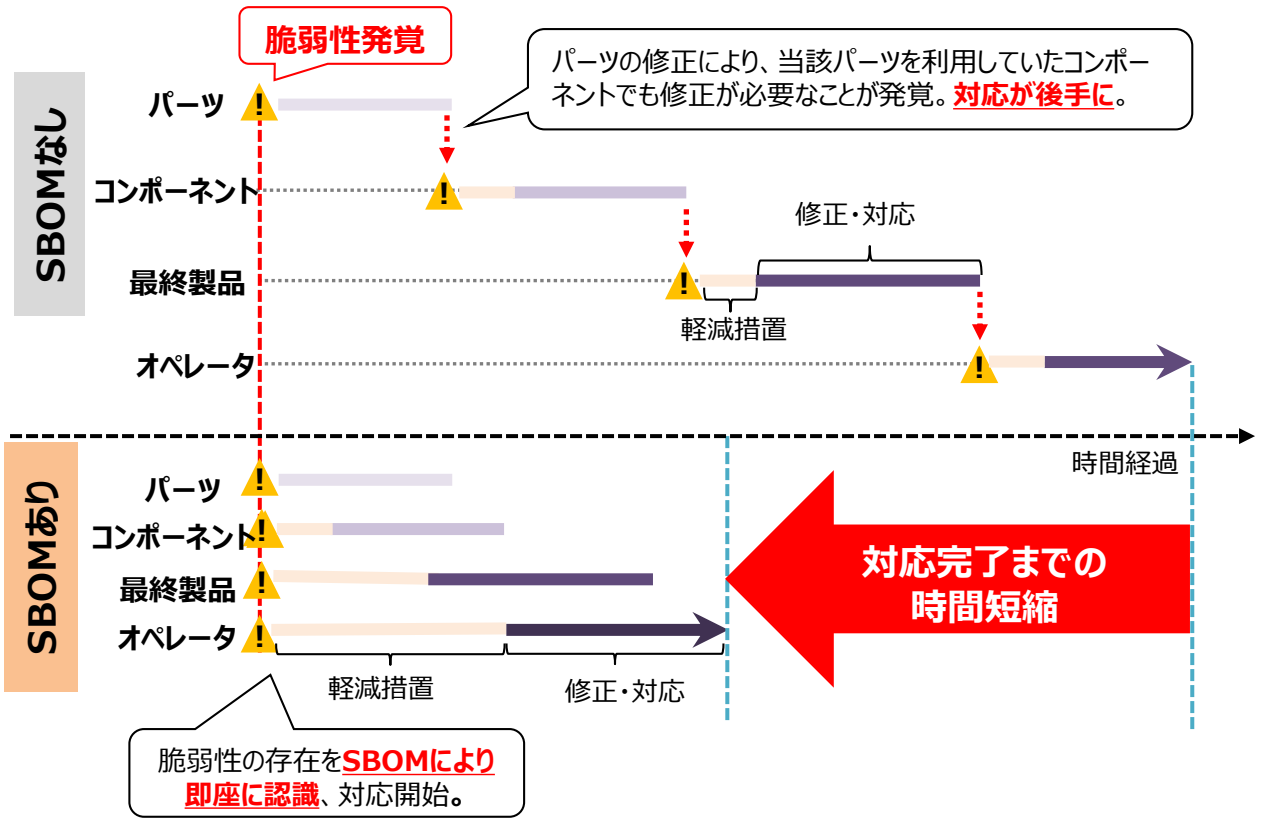
Component Name	Supplier Name	Version String	Author	Hash	UID	Relationship
Application	Acme	1.1	Acme	0x123	234	Self
|--- Browser	Bob	2.1	Bob	0x223	334	Included in
|--- Compression Engine	Carol	3.1	Acme	0x323	434	Included in
|--- Buffer	Bingo	2.2	Acme	0x423	534	Included in

https://www.ntia.doc.gov/SoftwareTransparency

ソフトウェアTF：SBOM活用に向けた実証

- ソフトウェアの成分構成を表す**SBOM（Software Bill of Materials）**を活用することにより、**ソフトウェアに何が含まれ、誰が作り、どのような構成となっているか**等の把握が容易になる。
- 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、自動車産業・電力分野にも取組が拡大。
- 日本においても業界構造や商習慣を考慮しつつ、SBOM活用に向けた実証事業の実施を検討。

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。

自動車産業分野

Auto-ISACを中心としたサプライヤ中心のプロジェクト。12ヶ月ほどかけてサプライヤの推奨事項をとりまとめる予定。

電力分野

1/26キックオフ。米国エネルギー省からもプレゼンターとして参加。

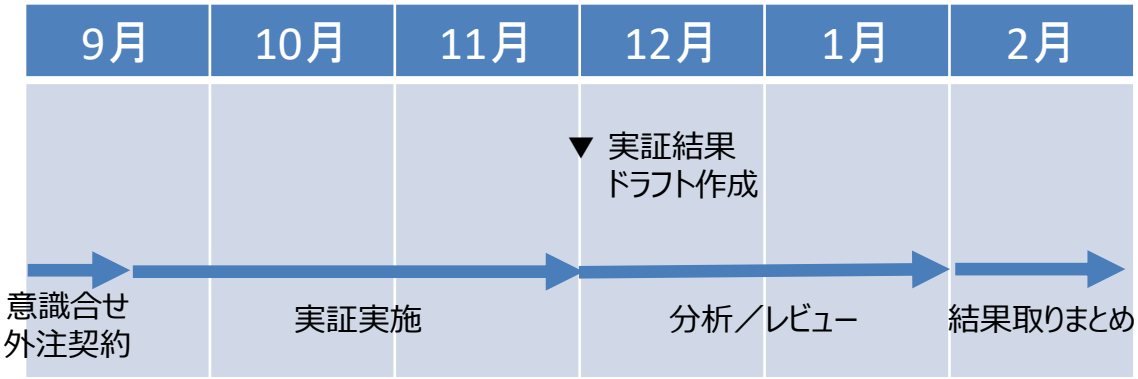
SBOM実証の対象ソフトウェア・体制・スケジュール

- 本年度は、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し、実証事業を実施**。

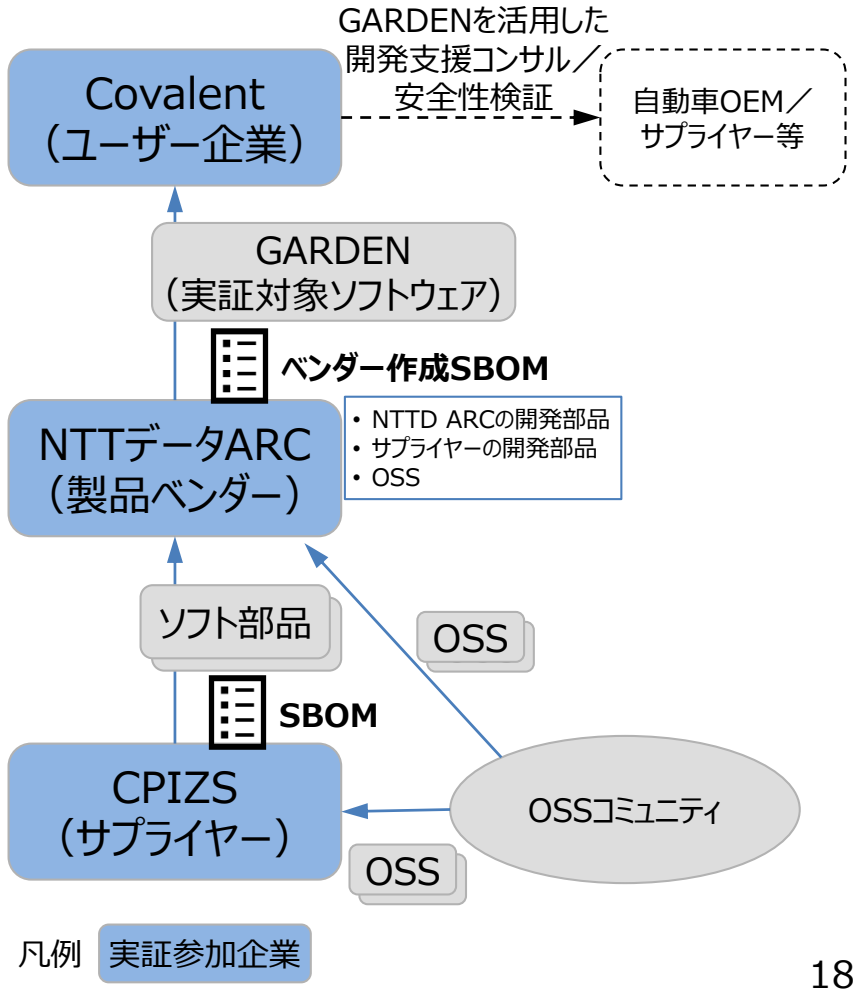
実証対象ソフトウェア 「GARDEN」

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）




METI
Ministry of Economy, Trade and Industry