TOSHIBA

OSSセキュリティ技術ワークショップ(OWS) 2023

SBOM
-オープンソースコンプライアンスなどリスクマネジメントの基礎となるもの。そして、その先へ -

株式会社 東芝
デジタルテクノロジーイノベーションセンター 戦略室
オープンソースプログラムオフィス (OSPO)
忍頂寺 毅
(Leader of Automation-SG, Co-Sub Leader of SBOM-SG, Japan-WG, OpenChain Project, Linux Foundation)

2023.10.31

Contents

01

はじめに

- 自己紹介
- 所属組織紹介

自己紹介

忍頂寺 毅 (ニンジョウジ タカシ)

シニアマネージャー
Head of Open Source Program Office (OSPO)

職歴

2020~ 現在	TOSHIBA	オープンソースの活用推進
2011~ 2020	DeNA	技術管理、リスクマネジメント
2001~ 2011	ドコモ	モバイルAR, HCI, 移動機端末
1998~ 2001	NTT	IPv6 関連

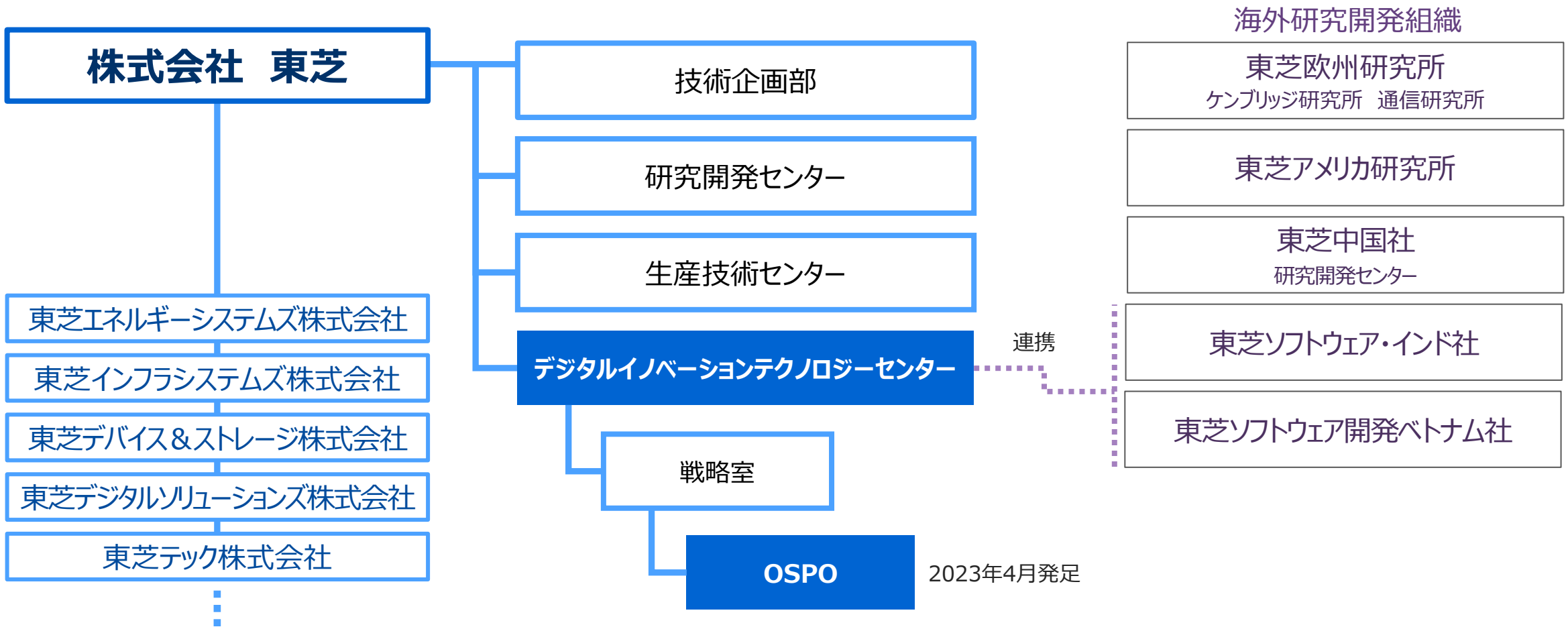
オープンソース関連活動

OpenChain Project (ボードメンバー)
Open Invention Network (OIN) (Technical Advisory Council (TAC))
(一) ソフトウェア情報センター (SOFTIC) (オブザーバ委員)

株式会社東芝 デジタルイノベーションテクノロジーセンター

※2023年4月1日現在

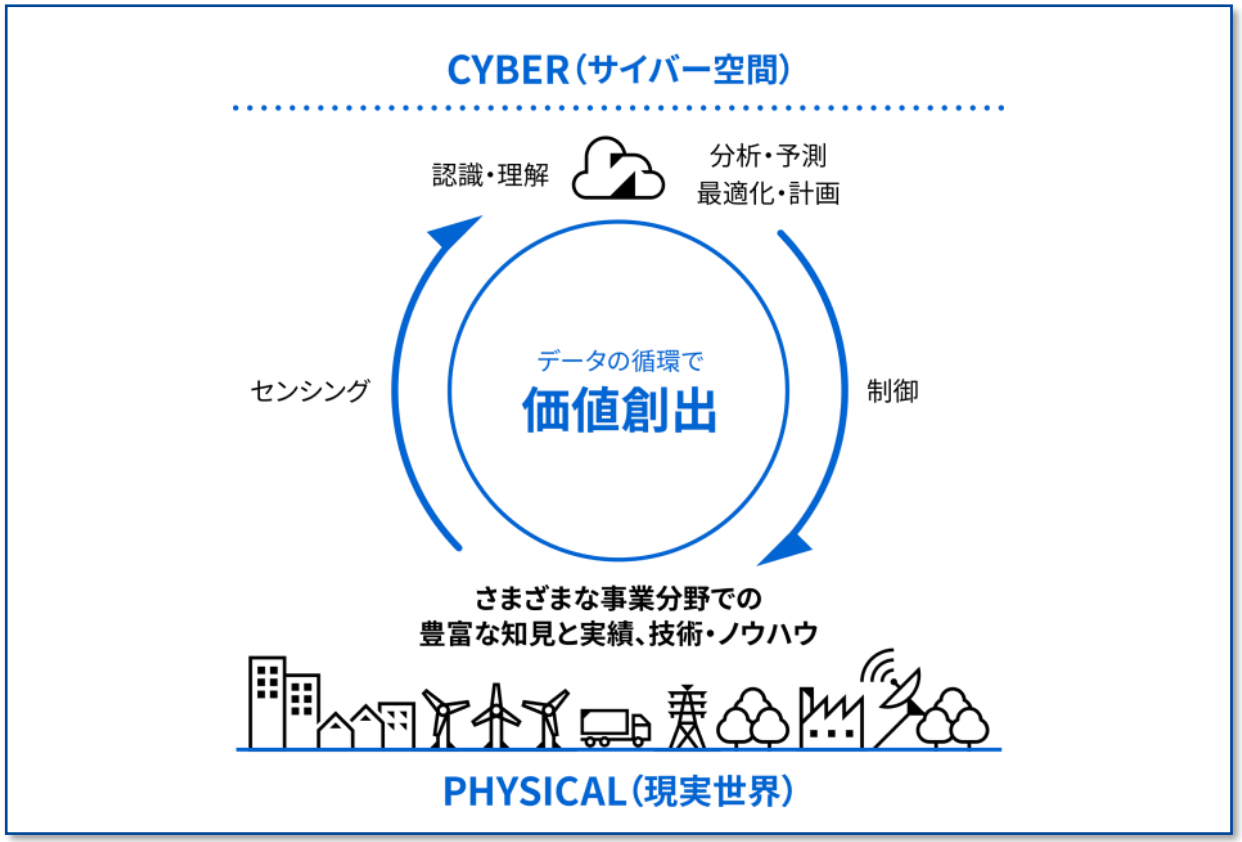
ソフトウェア開発およびソフトウェア開発技術で東芝グループを牽引する



Cyber Physical Systems (CPS) への取組

サイバー空間と現実世界がデジタルで連関し、価値を創造する

産業向けIoTやAIなどの最先端技術を活用した自動化・最適化のソリューションを提供



See also:「東芝のCPS」. https://www.global.toshiba/jp/cps/corporate.html

デジタルイノベーションテクノロジーセンター の主な技術領域

ビジネスを止めずに成長するためのソフトウェア関連技術

ソフトウェアエンジニアリング技術

システムエンジニアリング

CPS共通サービス向け基盤

効率化

共通要素技術

AI活用IoTサービスのための
MLOps基盤

デジタル化への適応力向上

共通ソフトウェア開発技術

ソフトウェア製品・
クラウドサービス技術

DX関連コア技術

東芝の OSPO (Open Source Program Office)

オープンソースとインナーソースの活用を推進する

利用やコンプライアンスの実施をステップに、コミュニティへの貢献を通じて、
オープンソースのエコシステムと共に成長する企業であり続ける

戦略・ガバナンス

- OSS/ISS 戦略の立案、推進
- エンジニアエンゲージメント (人材開発)

リスクマネジメント

- SBOM
- コンプライアンス
- ソフトウェア開発インフラ

教育・トレーニング

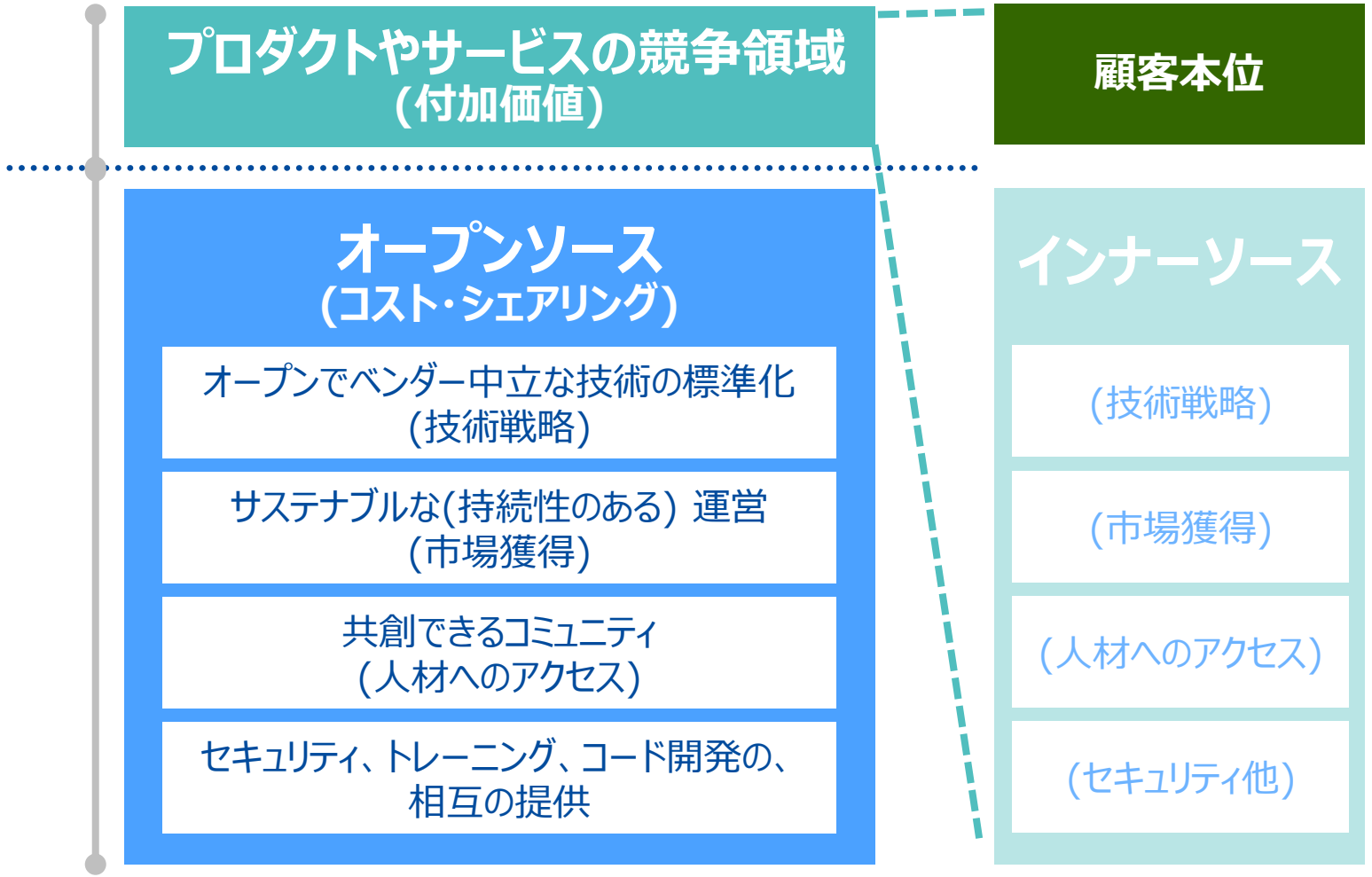
- オープンソース文化の浸透

標準化活動

- オープンソースコミュニティへの貢献

オープンソース, オープンアーキテクチャ, オープンスタンダード の重要性

オープンソースのエコシステムと事業とが共に成長していく必要がある



顧客価値向上にあたり、
特定依存の見極めが重要

技術標準の導入や、技術標準を主導し、当該技術に係る市場を成長させる

技術平準化による機動的な人材投入の素地を築く

Open Source Program Office (OSPO)

オープンソースの活用戦略に従って、ルール、プロセス、教育などの環境整備、関連部署との連携、コミュニティとの連携など、関連する活動をとりまとめ・支援する組織のこと

OSPO を設置する狙い

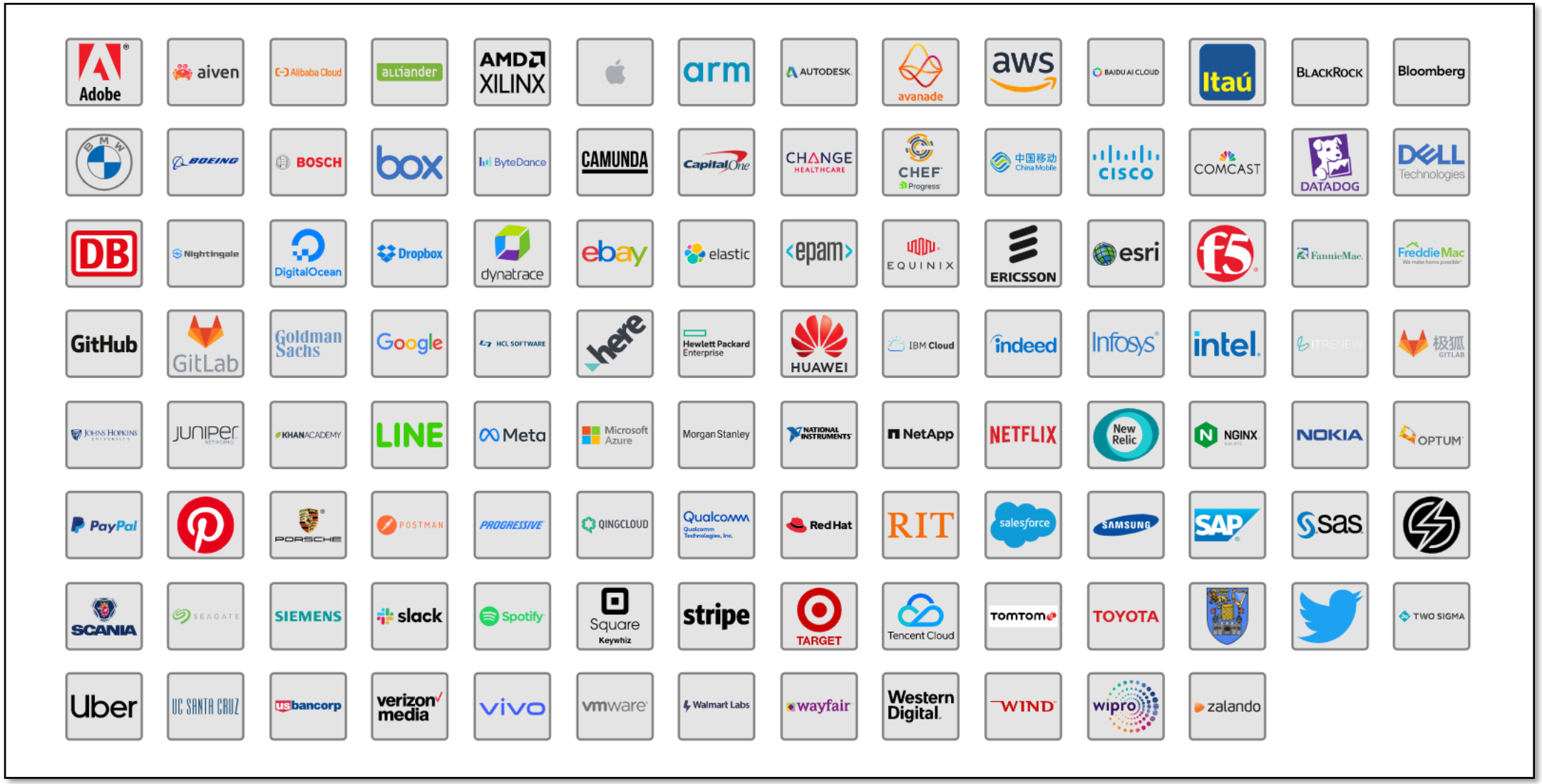
(1) 組織のオープンソース運用とその組織のコンピテンシーセンターになること。
(2) 組織のオープンソース活動の戦略と一連のポリシーを設定すること。
これには、コードの使用、配布、選択、監査などのポリシーの設定、開発者のトレーニング、法令遵守の確保、組織に戦略的利益をもたらすコミュニティへの参加促進とその構築などが含まれます。

OSPO の特徴

(1) 従業員は、OSS活用方法の育成と拡大を正規の業務としている。
(2) 組織は、OSSの使用、および製品化に関する正式なポリシーを有する。
(3) 経営幹部は、OSSと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。
(4) かなりの数の従業員がオープンソース プロジェクトにコードを提供している。
(5) オープンソースの利用と参加を効率化し、促進するためのプロセス、手順、ツールが整備されている。

出典：Ibrahim Haddad, A Deep Dive Into Open Source Program Offices, 2022. のLinux Foundation による日本語訳版。Licensed under the CC-BY-ND-4.0

【動向】OSPO導入企業の例



出典：Linux Foundation, OSPO Landscape, https://landscape.todogroup.org/

OSPO成熟度モデル

技術分野に応じてステージを使い分ける

02

東芝が参加するオープンソースプロジェクトの例

- Civil Infrastructure Platform
- OpenChain Project

東芝のオープンソース活動の例

インフラとソフトウェアサプライチェーンへの貢献

コンシューマプロダクトから始まり、インフラ向けのLinuxやコンプライアンスへ

2001 2006 2011 2016 2020

CE Linux Forum

▲ 2003
(joined)

The Linux Foundation

▲ 2010
CE Workgroup
(merged)

▲ 2016
Civil Infrastructure Platform
Platinum member
(initiated)

▲ 2018
OpenChain Project
Platinum member
(joined)

▲ 2015
Debian
Debian-LTS
(joined)

▲ 2019
Open Invention Network (OIN)
Technical Advisory Council
(joined)

THE LINUX FOUNDATION PROJECTS

Civil Infrastructure Platform

Industrial-Grade Linux

Urs Gleim, Siemens AG, CIP Board Chair
Yoshitake Kobayashi, Toshiba Corp., CIP TSC Chair
September, 2023

Establishing an

Open Source Base Layer

of industrial-grade software to enable the use and implementation of software building blocks for Civil Infrastructure Systems

CIVIL INFRASTRUCTURE PLATFORM

CIVIL INFRASTRUCTURE PLATFORM

Platinum members

RENESAS SIEMENS TOSHIBA

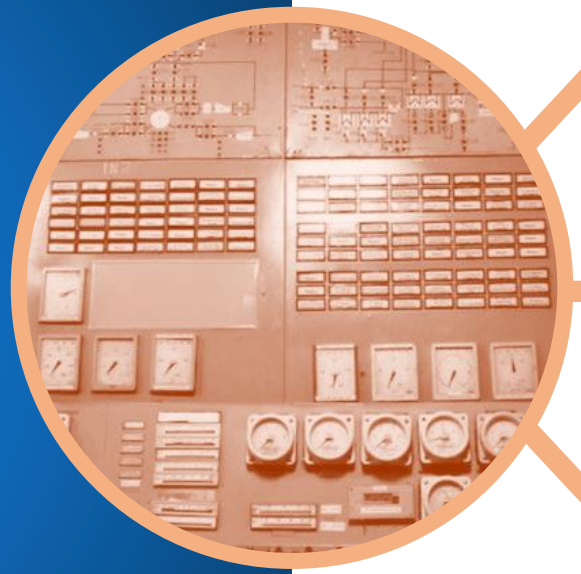
Silver members

BOSCH cybertrust HITACHI Inspire the Next

LINUTRONIX MOXA Plat'Home There, we are. Internet of Things

The key challenges

- Apply IoT concepts to industrial systems
- Ensure quality and longevity of products
- Keep millions of connected systems secure



Industrial gradeness

- Reliability
- Functional Safety
- Real-time capabilities

Sustainability

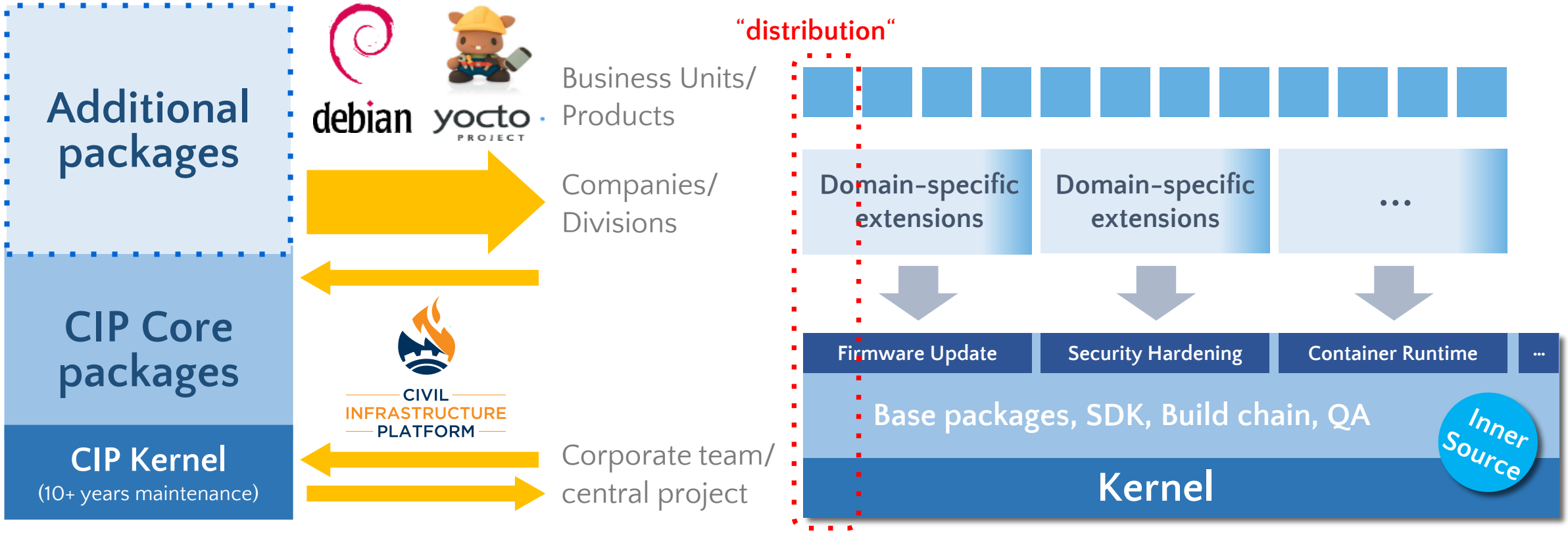
- Product life-cycles of decades
- Backwards compatibility
- Standards

Security

- Security & vulnerability management
- Firmware updates
- Minimize risk of regressions

CIVIL INFRASTRUCTURE PLATFORM

Mapping CIP into the company



Up to 70% effort reduction achievable for OSS license clearing and vulnerability monitoring, kernel and package maintenance, application adaptation and testing for an individual product.

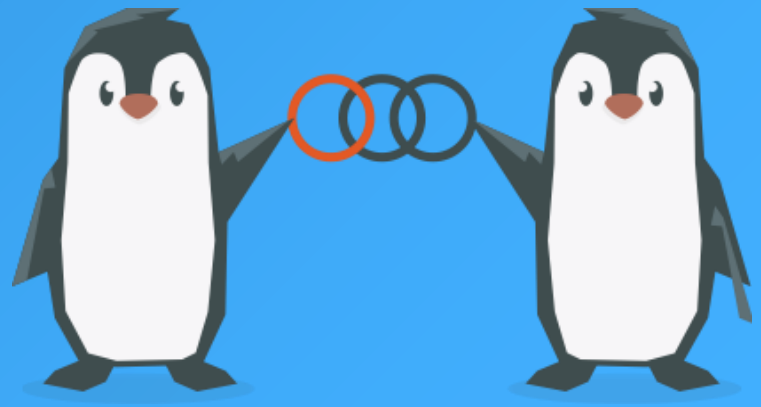
CIVIL INFRASTRUCTURE PLATFORM

OSS Open Source Software QA quality assurance SDK software development kit

The OpenChain Project

THE LINUX FOUNDATION

OPENCHAIN



OPENCHAIN

The OpenChain Projects builds standards to define the key requirements of quality open source license compliance and security assurance programs

These are simple, effective standards for organizations of all sizes in all markets. They are openly developed and freely available to all.

The OpenChain Project supports these standards with extensive reference material, free self-certification and a vibrant community:
https://www.openchainproject.org/get-started

THE LINUX FOUNDATION

OPENCHAIN

活動体制

Platinum Members

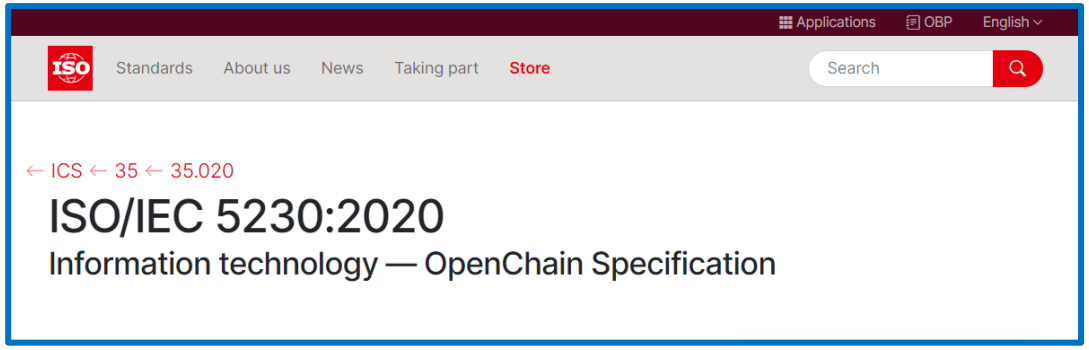
★ Governing Board Chair

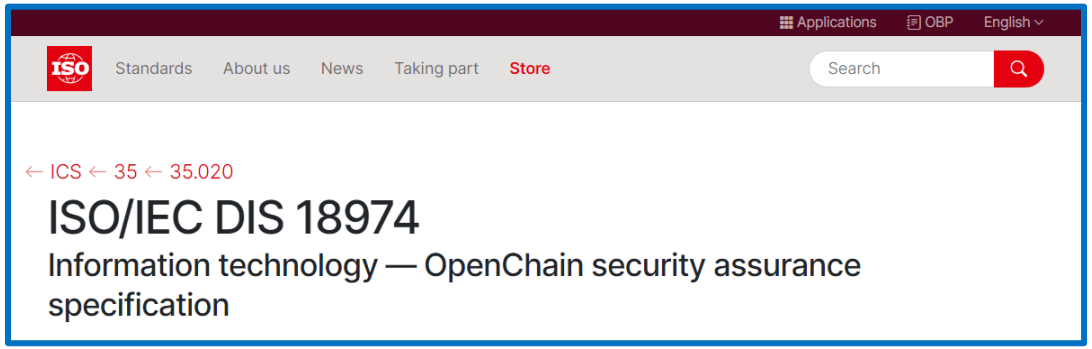
Community

- **Main Community:** https://lists.openchainproject.org/g/main
- **Automotive Work Group:** https://groups.io/g/openchain-automotive-work-group
- **Tooling Work Group:** https://groups.io/g/oss-based-compliance-tooling
- **Telco Work Group:** https://lists.openchainproject.org/g/telco
- **Education Work Group:** https://lists.openchainproject.org/g/education
- **Specification Development Discussions:** https://lists.openchainproject.org/g/specification
- **Partner Network:** https://lists.openchainproject.org/g/partners

標準化や、トレーニングコンテンツの提供など

プロセスマネジメントを国際標準化



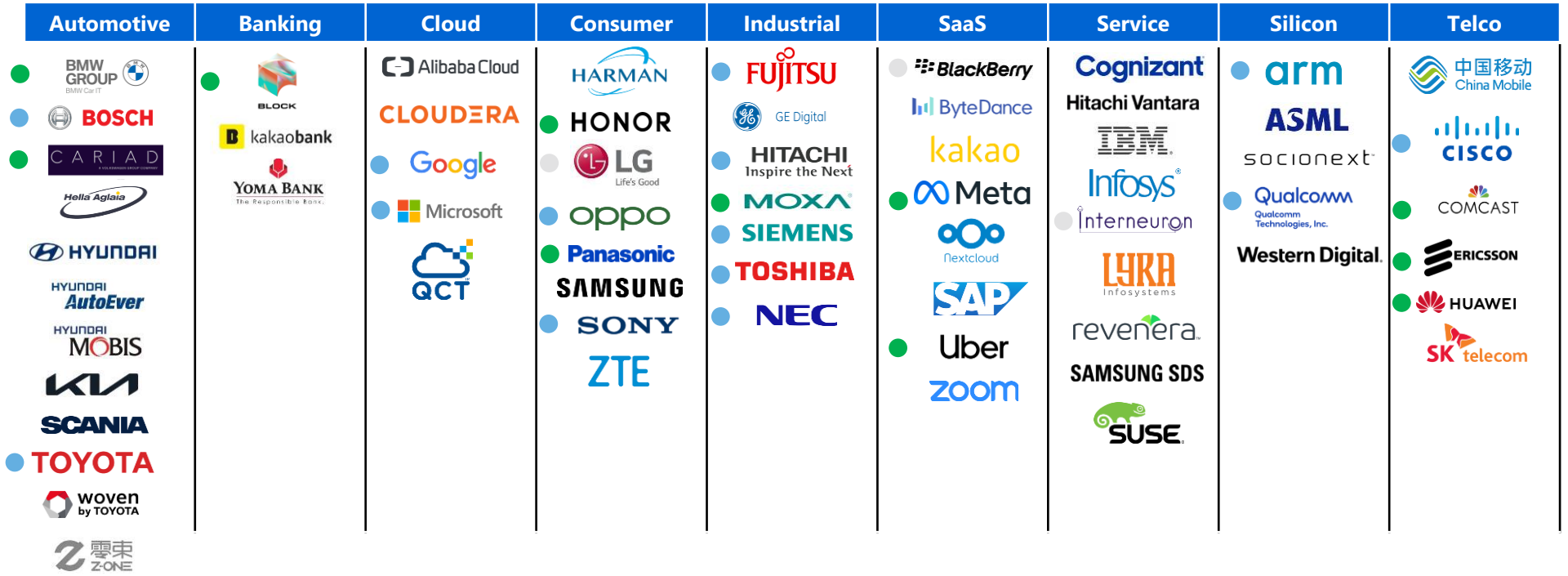


Linux Foundationのトレーニングコンテンツとして提供

THE LINUX FOUNDATION

OPENCHAIN

5230の適合事例：産業別



● Platinum Member / Conformance Pending ● Platinum Member + ISO/IEC 5230 Conformant ● ISO/IEC 5230 + DIS 18974 Conformant

This is a snapshot based on membership and select conformant organizations currently listed on our website. Total conformant numbers are far higher.
Example: PwC Survey shows 20% of companies in Germany with over 2,000 employees already used ISO/IEC 5230.

THE LINUX FOUNDATION

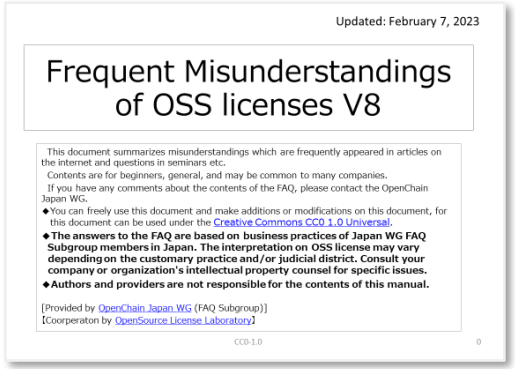
OPENCHAIN

Japan-WG

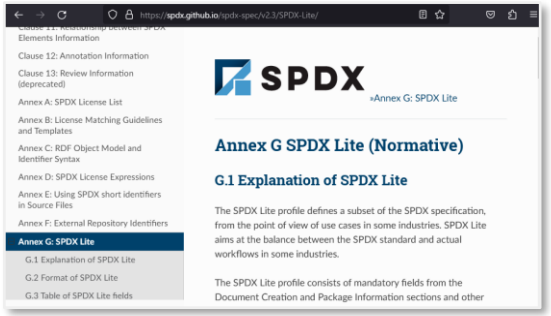
日本語で議論し、日本語／英語でアウトプット

A Supplier Education Guide For ISO/IEC 5230

FAQ of License Compliance based on business practices



SPDX Lite (Annex of SPDX Spec.)



https://openchain-project.github.io/OpenChain-JWG/

03

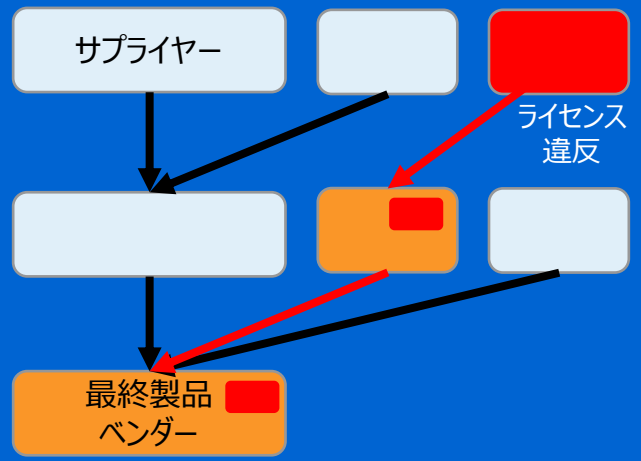
SBOM

オープンソースコンプライアンスやセキュリティアシュアランスなど、リスクマネジメントの基礎となるもの

背景：ソフトウェアサプライチェーンにおけるソフトウェア透明性の確保

【従来】ライセンスコンプライアンスやサイバーセキュリティの観点から、ソフトウェア部品表 (SBOM) の管理が必須
【現在】サイバーセキュリティ (脆弱性管理) の強化のため、SBOM管理を法的に要請する流れ

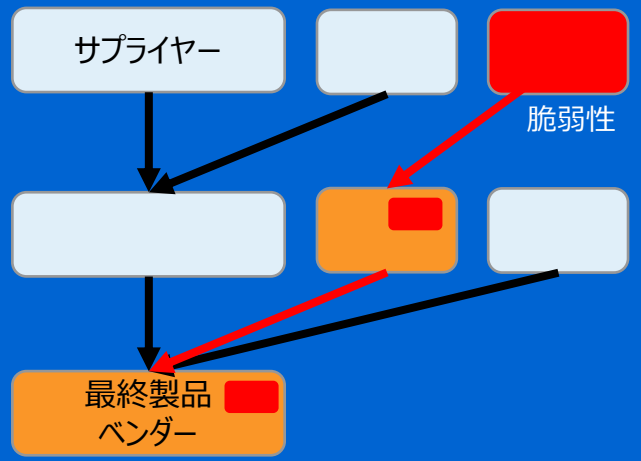
ライセンスコンプライアンス



E.g. GPL違反に基づく訴訟
BusyBox 訴訟 (2007-現在)、
FSF v. Linksys (Cisco) (2008-2009) 他

- OSPO (Open Source Program Office) を設置してオープンソース活用に取り組む企業が増えている
- オープンソースコンプライアンスのプロセスマネジメント標準 ISO/IEC 5230 (OpenChain Specification) がある

サイバーセキュリティ



E.g. バックドアや脆弱性を突いた攻撃
バックドア：SolarWinds (2020)
脆弱性　：OpenSSL(Heart Bleed, 2013)、
Apache Stratus2 (2017)、
Log4Shell (2021) 他

- SBOM管理に基づく脆弱性管理の取組が活発化
- オープンソースのセキュリティアシュアランスのプロセスマネジメント標準 ISO/IEC DIS 18974 (OpenChain Security Assurance Specification) の策定が進行中

各国動向

米国
連邦政府調達でSBOMの提供を推奨
- Executive Order 14028 (2021)
- Minimum Elements for SBOM、他

EU
デジタル製品で脆弱性とSBOMの管理を要求
- Cyber Resilience Act (CRA) (案)

日本
インフラの安定的な提供の確保
- 経済安全保障推進法
- サイバーセキュリティ基本法

医療機器
- IMDRF (International Medical Device Regulations Forum)
- FDA (U.S. Food & Drug Administration)

国内動向

経済産業省 産業サイバーセキュリティ研究会 WG1 配下のサイバー・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での検討や、関連する所管省庁の動きがある

基幹インフラ役務の対象分野[1]

電気	ガス	石油
水道	鉄道	貨物 自動車 輸送
外航 貨物	航空	空港
電気 通信	放送	郵便
金融	クレジット カード	

重要インフラ分野[2]

電力	ガス	石油
水道	鉄道	物流
	航空	空港
情報 通信	医療	政府・行政 サービス*
金融	クレジット カード	化学

KDDIが通信分野のSBOM導入の実証実験を開始[3]

（* 地方公共団体を含む）

1. 内閣府.「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（経済安全保障推進法）」. https://www.cao.go.jp/keizai_anzen_hosho/index.html
2. 内閣サイバーセキュリティ―センター.（重要インフラグループ）「グループの概要」. https://www.nisc.go.jp/policy/group/infra/index.html
3. KDDI. ニュースリリースより. https://news.kddi.com/kddi/corporate/newsrelease/2023/08/01/6897.html

ISO/IEC 5230 及び ISO/IEC RPF 18974 での SBOM の扱い

リスクマネジメントの基礎として必須となっている

5230 Requirements	
1. Program foundation	1.1 Policy
	1.2 Competence
	1.3 Awareness
	1.4 Program scope
	1.5 License obligations
2. Relevant tasks defined and supported	2.1 Access
	2.2 Effectively resourced
3. Open Source content review and approval	3.1 Bill of Materials
	3.2 License compliance
4. Compliance artifact creation and delivery	4.1 Compliance artifacts
5. Understanding open source community engagements	5.1 Contributions
6. Adherence to the specification requirements	6.1 Conformance
	6.2 Duration

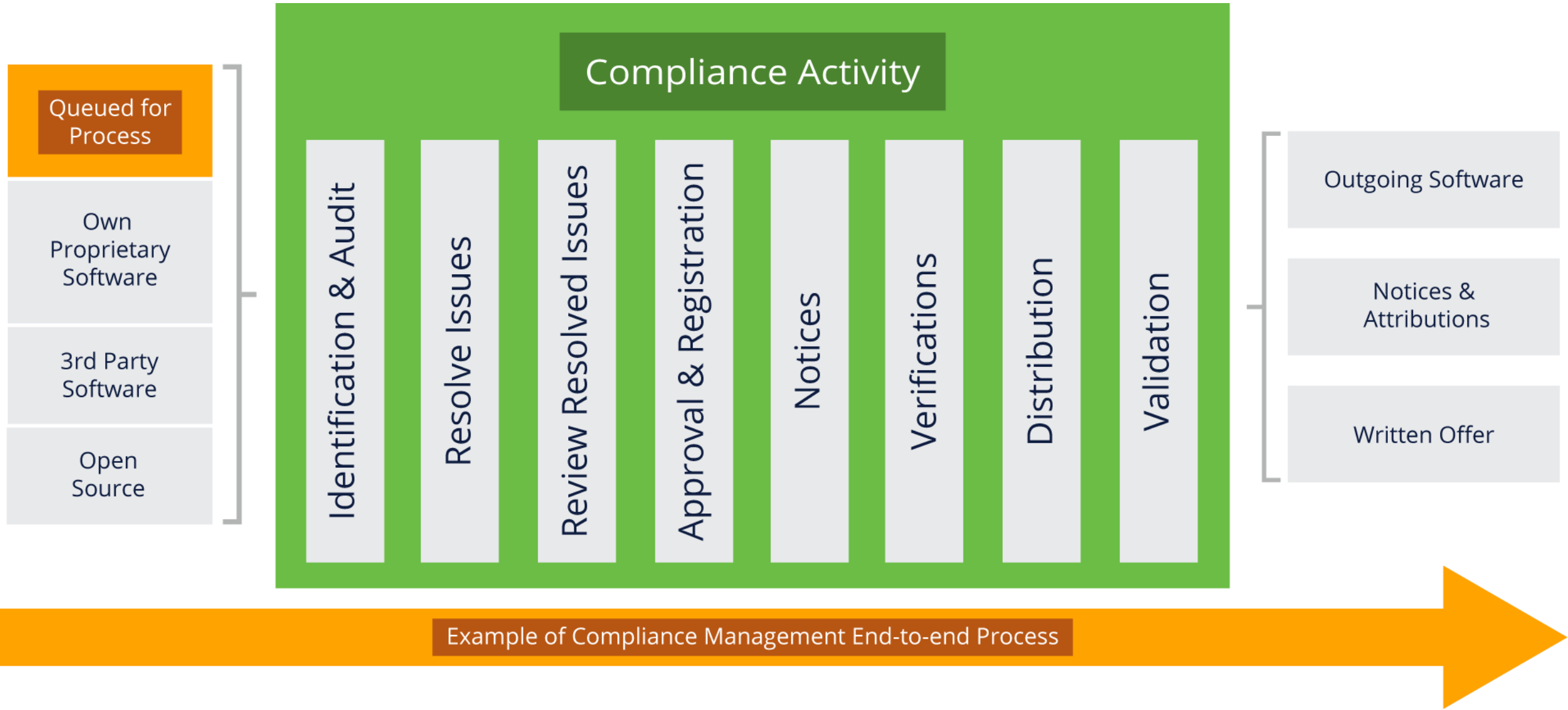
18974 Requirements	
1. Program foundation	1.1 Policy
	1.2 Competence
	1.3 Awareness
	1.4 Program Scope
	1.5 Standard Practice Implementation
2. Relevant tasks defined and supported	2.1 Access
	2.2 Effectively resourced
3. Open Source content review and approval	3.1 Software Bill of Materials (SBOM)
	3.2 Security Assurance
4. Adherence to the guideline requirements	4.1 Completeness
	4.2 Duration

ISO/IEC 5230:2020 (OpenChain Specification)

- どのようなソフトウェアコンポーネントを利用しているかを明らかにし、レビューと承認を得て、事業に供することを要求する
- ライセンスのユースケースに応じた取り扱いに関して文書化された手順がある

3.1	**プログラムの基盤**	
3.1.1	ポリシー	OSSポリシーを定め、プログラム参加者に周知している
3.1.2	力量	プログラム参加者の力量を定め、トレーニングやエビデンスを管理する
3.1.3	認識	プログラム参加者が、ポリシーなどについて、プログラムにおける役割と責任を果たす程度に十分な認識の水準を有している
3.1.4	プログラムの適用範囲	プログラムの適用範囲を明確にしている、
3.1.5	ライセンス義務	ライセンスを確認し、レビューするためのプロセスがある
3.2	**関連業務の定義と支援**	
3.2.1	アクセス	第三者からのOSSに関する問い合わせ窓口と対応手順のためのプロセスが明確である
3.2.2	十分なリソース配分	プログラム参加者の役割を定義し、必要なリソースを割り当てている（法律の専門家が関わるようになっている）
3.3	**オープンソースコンテンツのレビューと承認**	
3.3.1	部品表 (Bill of Materials)	SBOMの管理プロセスがあり、供給ソフトウェアに関するSBOMを記録管理する
3.3.2	ライセンスコンプライアンス	バイナリ形式での配布の場合など、利用の実施態様に応じた手順がある
3.4	**コンプライアンス関連資料の作成と頒布**	
3.4.1	コンプライアンス関連資料	ライセンスのコンプライアンスに必要な成果物を明確にし、管理している
3.5	**オープンソースコミュニティ活動への理解**	
3.5.1	コントリビューション	コミュニティへ貢献するポリシーを定め、組織に周知し、所定のプロセスを実施している
3.6	**仕様要求事項の遵守**	
3.6.1	適合	ISO/IEC 5230 への適合を監査している
3.6.2	期間	適合取得から過去18か月以内で、すべての要求事項を満たしている

企業におけるライセンスコンプライアンスのプロセス例



出典：Implementing Open Source License Compliance Management (LFC194)

ISO/IEC RPF 18974 (OpenChain Security Assurance Specification)

- どのようなソフトウェアコンポーネントを利用しているかを明らかにし、レビューと承認を得て、事業に供することを要求する
- 脆弱性を検出し解決する場合のプロセス文書があり、対応時の記録管理を実施する

4.1	**プログラムの基盤**	
4.1.1	ポリシー	オープンソースセキュリティアシュアランスのポリシーを定め、プログラム参加者に周知している
4.1.2	力量	プログラム参加者の力量を定め、トレーニングやエビデンスを管理する
4.1.3	認識	プログラム参加者が、ポリシーなどについて、プログラムにおける役割と責任を果たす程度に十分な認識の水準を有している
4.1.4	プログラムの適用範囲	プログラムの適用範囲を明確にしている、
4.1.5	標準プラクティスの実装	脆弱性の対処やセキュアなソフトウェア開発のための手順がある
4.2	**関連業務の定義と支援**	
4.2.1	アクセス	脆弱性に関する第三者からの問い合わせ窓口と対応手順などのプロセスが明確である
4.2.2	十分なリソース配分	プログラム参加者の役割を定義し、必要なリソースを割り当てている (脆弱性に関する技術専門家が関わるようになっている)
4.3	**オープンソースソフトウェアコンテンツのレビューと承認**	
4.3.1	ソフトウェア部品表	SBOM (Software Bill of Materials)の管理プロセスがあり、供給ソフトウェアに関するSBOMを記録管理する
4.3.2	セキュリティアシュアランス	供給ソフトウェアのSBOMにあるオープンソースソフトウェア部品について、セキュリティアシュアランスのためのプロセスがある
4.4	**仕様要求事項の遵守**	
4.4.1	適合	ISO/IEC 18974 への適合を監査している
4.4.2	期間	適合取得から過去18か月以内で、すべての要求事項を満たしている

Software Bill of Materials (SBOM) の定義

およそ、Executive Order 14028 をベースに定義しているようにみられる

国	概要
US(1)(2)	a formal record containing the details and supply chain relationships of various components used in building software
EU(3)(4)	a formal record containing details and supply chain relationships of components included in the software elements of a product with digital elements
日本(5)	ソフトウェアコンポーネントやそれらの依存関係の情報も含めた機械処理可能な一覧リストのこと

(1) Whitehouse. “Improving the Nation's Cybersecurity”. Executive Order 14028 of May 12, 2021
Retrieved from: https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity
(2) NTIA. “The Minimum Elements For a Software Bill of Materials (SBOM)”
Retrieved from: https://www.ntia.gov/report/2021/minimum-elements-software-bill-materials-sbom
(3) European Commission. “Cyber Resilience Act”
Retrieved from: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act
(4) Council of the European Union. “Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/102”
Retrieved from: https://data.consilium.europa.eu/doc/document/ST-12536-2023-INIT/en/pdf
(5) 経済産業省.「ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引 Ver. 1.0」
Retrieved from: https://www.meti.go.jp/press/2023/07/20230728004/20230728004.html

NTIA. The Minimum Elements For Software Bill of Materials (SBOM) (発行：2021.06.12)

E.O. 14028 を受けて、ソフトウェアサプライチェーンにおけるソフトウェア部品の透明性を確保するため、SBOM の管理のための最低限の項目を示す

主要な論点は次の3つ

1. Data Field (後述)

2. Automation Support

- 自動で生成し処理でき、Machine-readable (機械可読性)であること
- Human-readable (人可読性)でもあるデータフォーマットを利用し、相互互換を図ること
  - **Software Package Data eXchange (SPDX)**
  - **CycloneDX**
  - **Software Identification (SWID) tags**

3. Practice and Processes

- 頻度 (ソフトウェアの構成に変化がある都度、SBOMを更新すること→**最新の状態のSBOMを管理**すること)
- 深さ (**最善は全ての依存関係**の網羅。**最小の場合は primary (top-level)** のコンポーネントを明らかにすること。再帰的に追跡して検証できる程度には必要。)
- Known Unknowns (依存関係の存在を明確にすること)
- 配布と納品 (SBOMをサプライチェーンで共有すること)
- **アクセスコントロール** (必要に応じて秘密情報として扱うこと)
- **間違いの許容** (SBOM管理についてリスク管理の観点では発展段階にあること)

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

Software Bill of Materials (SBOM) の構成に関する動向

“The Minimum Elements of Software Bill of Materials” が一定の目安にはなっている

国	概要
US(1)	1. Data Field としての最小限の要素を明らかにする (後述) 2. 最善は全ての依存関係の網羅、最小の場合はprimary (top-level) のコンポーネントを全て
EU(2)(3)	1. 欧州委員会がSBOMの情報構成要素を定める権限持つ (法案において。詳細不明) 2. 少なくとも、その製品の最上位レベルの依存関係
日本(4)	USが公開済みの文書の紹介や、SPDXなどSBOMのデータフォーマットの例示などに留まる

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

(2) European Commission. “Cyber Resilience Act“
Retrieved from: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

(3) Council of the European Union. “Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/102“
Retrieved from: https://data.consilium.europa.eu/doc/document/ST-12536-2023-INIT/en/pdf

(4) 経済産業省.「ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引 Ver. 1.0」
Retrieved from: https://www.meti.go.jp/press/2023/07/20230728004/20230728004.html

Data Field: NTIA. Minimum Elements For SBOM

ソフトウェアコンポーネントを「特定」できるための最低限の情報

SBOM Minimum Field	Description （説明）
Author of SBOM Data（SBOMの作成者）	SBOM記載事項の作成者（サプライヤーとは限らない）
Timestamp（タイムスタンプ）	SBOMデータを作成した日時の記録
Supplier Name（サプライヤー名）	SBOM記載事項にあるコンポーネントの提供者の名称又は識別情報
Component Name（コンポーネント名）	オリジナルのサプライヤーが定めたソフトウェア単体の名称
Version of the Component（コンポーネントのバージョン）	コンポーネントを識別するためのバージョン
Other Unique Identifiers（その他の一意な識別子）	コンポーネントの識別や関連するデータベースのルックアップキーとして利用できるユニークな識別情報 → 脆弱性情報の検索に利用することが主に想定される。CPEやPURLなど。
Dependency Relationship（依存関係）	上流コンポーネントXがソフトウェアYに含まれる関係性の特徴 (“included”)

※上記は “The Minimum Elements For a Software Bill of Materials (SBOM)” の記載に基づくが、表の列記順は必ずしも一致しない

Data Field: NTIA. Minimum Elements For SBOM (cont.)

最低限のものに加えて、推奨されるデータフィールド

SBOM Minimum Field	Description （説明）
Component Hash （コンポーネントのハッシュ値）	コンポーネントをユニークに識別するための暗号化ハッシュ値 → 改変や改竄の有無の検証に有用と考えられる ※ 内部的には承認済みのコンポーネントとの照合にも利用できる
Lifecycle Phase （ライフサイクルの段階）	ソフトウェア開発ライフサイクルのどの段階 (“stage”とも)かを示す → ソースコード、ビルド用、ビルド後、リリース後、などでソフトウェア構成が変化することがありえるため Ex1. オリジナルのソースコードにテストコードを含むが、リリース時に含めない場合 Ex2. テスト中はデバッグ用のライブラリを含むが、リリース時に含めない場合 ※上記に限らない
Other Component Relationships （その他のコンポーネントとの関係）	コンポーネント間の関係 ※” Minimum Elements For SBOM” では、直接的な依存関係にはないコンポーネント同士の関係を表現する場合として、“derivation” (派生) や “descendancy” (後継/改良) などを例示する。これは、オリジナルに変更が加えられていることを示すため、共通の起源やその内容の追跡に有用だと指摘する。
License Information （ライセンス情報）	コンポーネントに適用されるライセンスに関する情報 → 利用者がリーガルリスクの有無を検証するために利用できる

Data Field: オープンソースコンプライアンスコミュニティの意見

取得手段の明示があると、利用側でも追加で検証できる

SBOM Minimum Field	Description （説明）
Download Location	コンポーネントを取得するための手段 → インターネット上のロケーション → バージョン管理システム (VCS。Gitなど) でのポインター、その他

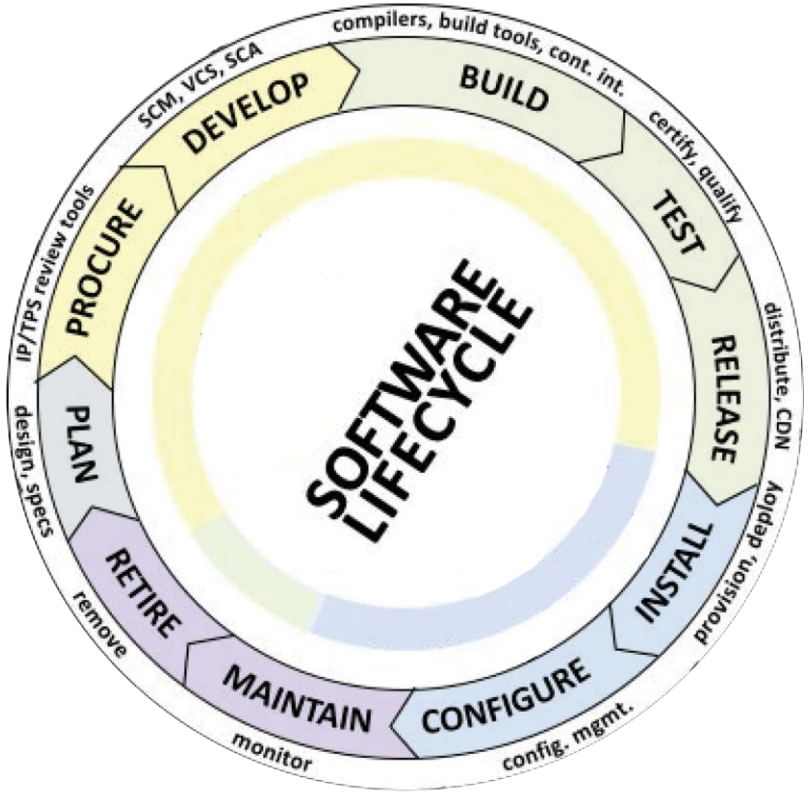
SBOMとSDLCとの関係

SBOM にはSDLCに応じたステージが考えられる

Source SBOM

Design SBOM

Runtime SBOM



Build SBOM

Deployed SBOM

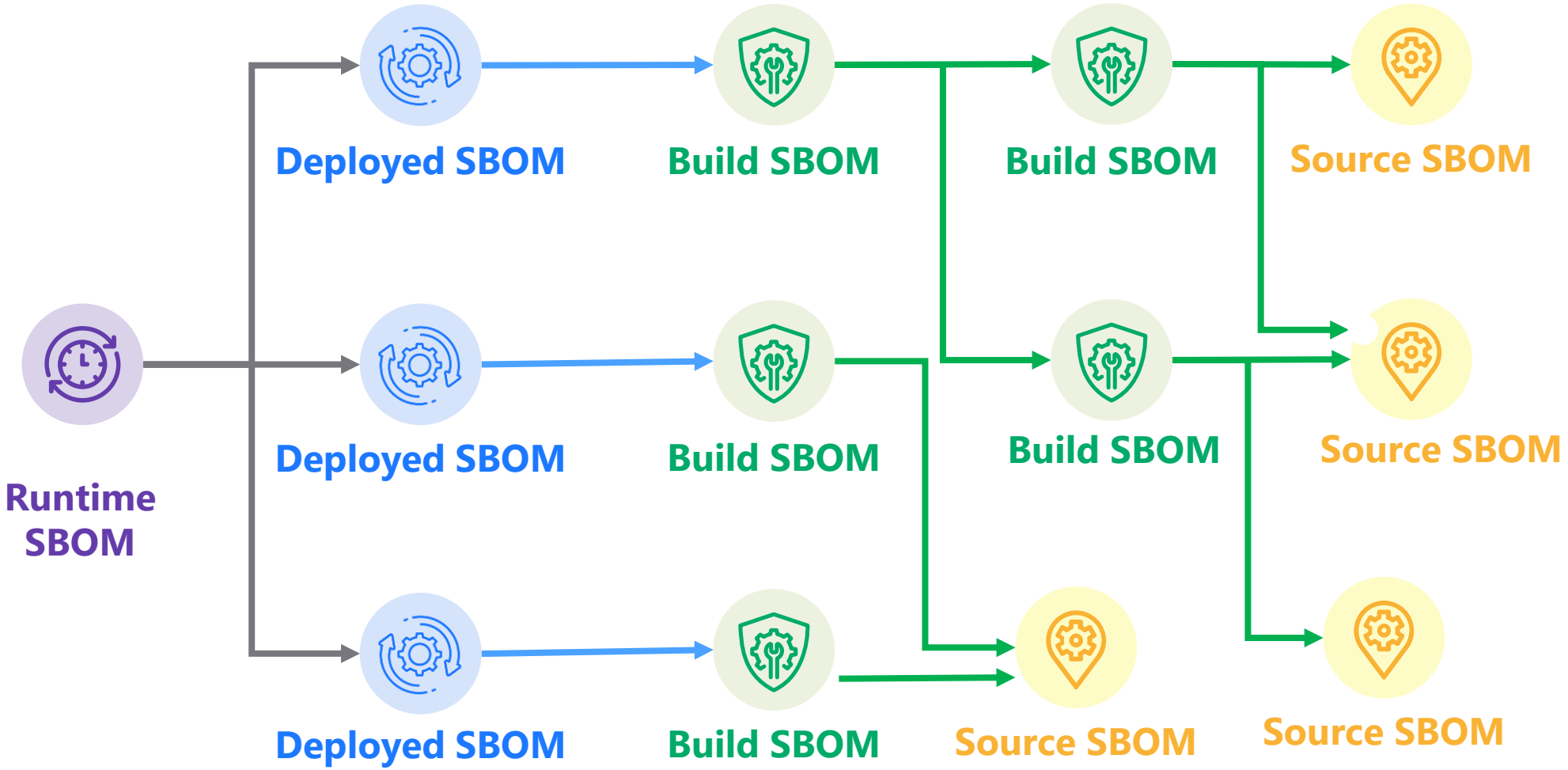
Source: Types of Software Bills of Materials (SBOM) published by CISA on 2023/4/21

SBOM Type Definition and Composition

SBOM Type	Definition	Data Description
Design	ソフトウェアのデザインや企画段階でのSBOM (机上検討時などコンポーネントの実際の有無に関わらず構成される)	仕様書やRFPなどに基づいて生成される
Source	ビルド前のソースコードや、ビルドで利用するために依存するコンポーネントを含むように作成したSBOM	ソフトウェア構成解析 (SCA) ツールの出力や、必要に応じて手作業で作成・修正した情報に基づいて生成される
Build	リリースされるソフトウェアのビルドプロセスで生成されるSBOM。 (実行時バイナリがターゲットとなる場合、ソースコード、依存するコンポーネント、ビルドコンポーネント、ビルド時のみ用いるデータ、その他関連するSBOMなど)	Source SBOM とビルドプロセスで必要となる情報に基づいて生成される。
Deployed	システムに存在するソフトウェアに関するインベントリー覧としてのSBOM (デプロイ環境に応じて利用するソフトウェアやコンフィギュレーションの組み合わせなどで構成される。たとえば、他のBuild SBOMとの組み合わせなどが想定される。)	システムにインストールされる際のSBOMとそのコンフィギュレーション情報の記録に基づいて生成される。
Runtime	ソフトウェアをシステムで稼働させたときの、システム全体のSBOM (動的に呼び出して利用するようなコンポーネントがある場合は “instrumented” SBOM または “Dynamic” SBOM として、システムを構成するSBOMとして管理する)	システムの実行環境に沿って、システムで実際に稼働するソフトウェアの記録に基づいて生成される。
Analyzed	解析して生成されたSBOM (実行バイナリ、パッケージ、コンテナ、仮想マシンイメージ を解析した結果などが想定される)	サードパーティ製の解析ツールの出力などに基づいて生成される。 ここで解析ツールとは、バイナリ解析ツールなどが想定される。

CISA. Types of Software Bill of Material (SBOM) Documents. から抄訳
https://www.cisa.gov/sites/default/files/2023-04/sbom-types-document-508c.pdf

Traceability



SBOMの主要なデータフォーマット

オープンソースコミュニティでは、SPDX や CycloneDX が話題になりやすい

名称	SPDX	CycloneDX	SWID
開発主体	SPDX Workgroup (Linux Foundation)	OWASP	NIST
最新のリリース年 (最初のリリース年)	2022 (2011)	2023 (2017)	2015 (2009)
最新のバージョン	2.3	1.5	ISO/IEC 19770-2:2015
主な策定の経緯	ライセンスコンプライアンス	セキュリティアシュアランス	ソフトウェア資産管理 (SAM)
概要	ソフトウェアコンポーネントについて、パッケージ、ファイル、スニペットの粒度で扱える。 国際標準規格 ISO/IEC 5962:2021は、V2.2.1に基づいている。V2.3では、NTIA の 最小要素への対応のための明確化がなされている。SBOMへの多様化するニーズに対応するため、プロファイルという概念を導入するV3.0仕様の検討が進んでいる。	コンポーネント間の関係や、ソフトウェアが呼び出す可能性がある外部APIとの関係といった、ソフトウェアとサービスのデータの流れなども扱える。脆弱性情報を扱うこともできる。V1.5では、 Machine Learning Bill of Materials (ML-BOM) Manufacturing Bill of Materials (MBOM)、Kubernetes Bill of Materials（KBOM) が新しく導入された。	ソフトウェア製品の一意の識別子を定めるものとして策定された。2009 年にISO/IECで国際標準化される。この仕様は有償で提供されているが、 NISTがガイドを一般公開している*。
対応するフォーマット	JSON、YAML、CVS (spreadsheet,XLX/XLSX)、Tag-Value、RDF/XMLなど	JSONやXMLなど	XML

* NIST Internal Report (NISTIR) 8060. “Guidelines for the Creation of Interoperable Software Identification (SWID) Tags” https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8060.pdf

SPDX v2.3

SPDX : SPDX Workgroup が策定するフォーマット (https://spdx.github.io/spdx-spec/v2.3/)

V2.2.1 は ISO/IEC 5962:2021 として国際標準化

E.O.14028や関連するNTIAのガイドラインを受けて、V2.3に改訂

Claus	Category	Tag
6	Document Creation Information	**(6.1) SPDX Version** **(6.2) Data License** **(6.3) SPDX Identifier** **(6.4) Document Name** **(6.5) SPDX Document Namespace** (6.6) External document reference (6.7) License list version **(6.8) Creator** **(6.9) Created** (6.10) Creator comment (6.11) Document comment
7	Package Information	**(7.1) Package Name** **(7.2) Package SPDX Identifier** **(7.3) Package Version** **(7.4) Package File Name** **(7.5) Package supplier (★)** (7.6) Package originator **(7.7) Package Download Location** **(7.8) Files Analyzed** (7.9) Package Verification Code (7.10) Package Checksum **(7.11) Package Home Page** (7.12) Source information **(7.13) Concluded License** (7.14) All Licenses Information from files **(7.15) Declared License** **(7.16) Comments on License** **(7.17) Copyright text** (7.18) Package summary description (7.18) Package detailed description **(7.20) Package Comment**

Claus	Category	Tag
7	Package Information	**(7.21) External Reference (★)** (7.22) External Reference comment (7.23) Package attribution text (7.24) Primary Package Purpose (7.25) Release Data (7.26) Built Date
8 (抜粋)	File Information	(8.1) File Name (8.2) File SPDX Identifier (8.4) File Checksum (8.5) Concluded License (8.6) License Information in File (8.8) Copyright Text
9 (抜粋)	Snippet Information	(9.1) Snippet SPDX Identifier (9.2) Snippet from File SPDX Identifier (9.3) Snippet Byte Range (9.5) Snippet Concluded License (9.8) Snippet Copyright Text
10 (抜粋)	Other Licensing Information Detected	**(10.1) License Identifier** **(10.2) Extracted Text** **(10.3) License Name** **(10.5) License Comment**
11 **(抜粋)**	Relationship between SPDX Elements Information	(11.1) Relationship
Annex F	External Repository Identifiers	外部参照先として利用される情報をまとめる
Annex G	SPDX Lite	パッケージ単位でSBOMを管理運用するためのプロファイル v2.0 から仕様入り
Annex H	SPDX File Tags	FSFE (Free Software Foundation Europe)が提唱する REUSE 記法 に基づく著作権及びライセンスの表示例

※黄色ハイライトは、Minimum Element 対応項目
※ Tagの**太字**は、SPDX Lite で扱う項目

V2.3での主な変更点

Clause 7 他
- License 関連は 全てOptional に変更。

Annex. F「External repository identifiers」
- 脆弱性管理のために “advisory” “fix” “url” などを追加。
- SBOMフォーマットにSWID を追加
- 参照サイトに gitoid (https://gitbom/dev) を追加。

Annex. G「SPDX Lite」
- NTIA minimum elements for SBOM への対応のために (7.5) Package Supplierと、脆弱性管理のために (7.21) External Reference を追加 (左表の★)

Annex. H「SPDX File Tag」
- REUSE 記法を Snippet にも適用する

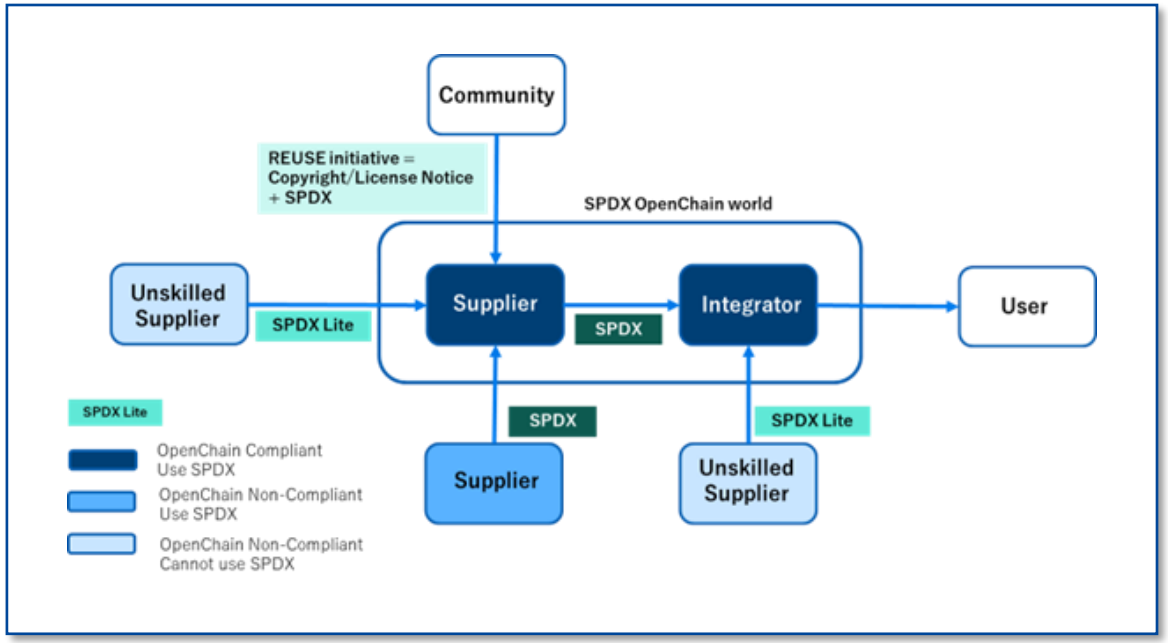
※ 2.3仕様検討以外のトピック

Build
- build 時の SBOM 生成に関する検討 (OpenSSF や CNCF のメンバーと協力)

3.0
- 他のBOMを包括しうるモデルの検討

SPDX Lite (Annex G of SPDX v2.x)

- SPDX仕様のサブセットであり、ライセンスコンプライアンスのための最小限の要素を定めたもの
- 設計方針はISO/IEC 5230 及び 同 PRF 18974 のプロセスといった実務で使いやすい明快な情報管理



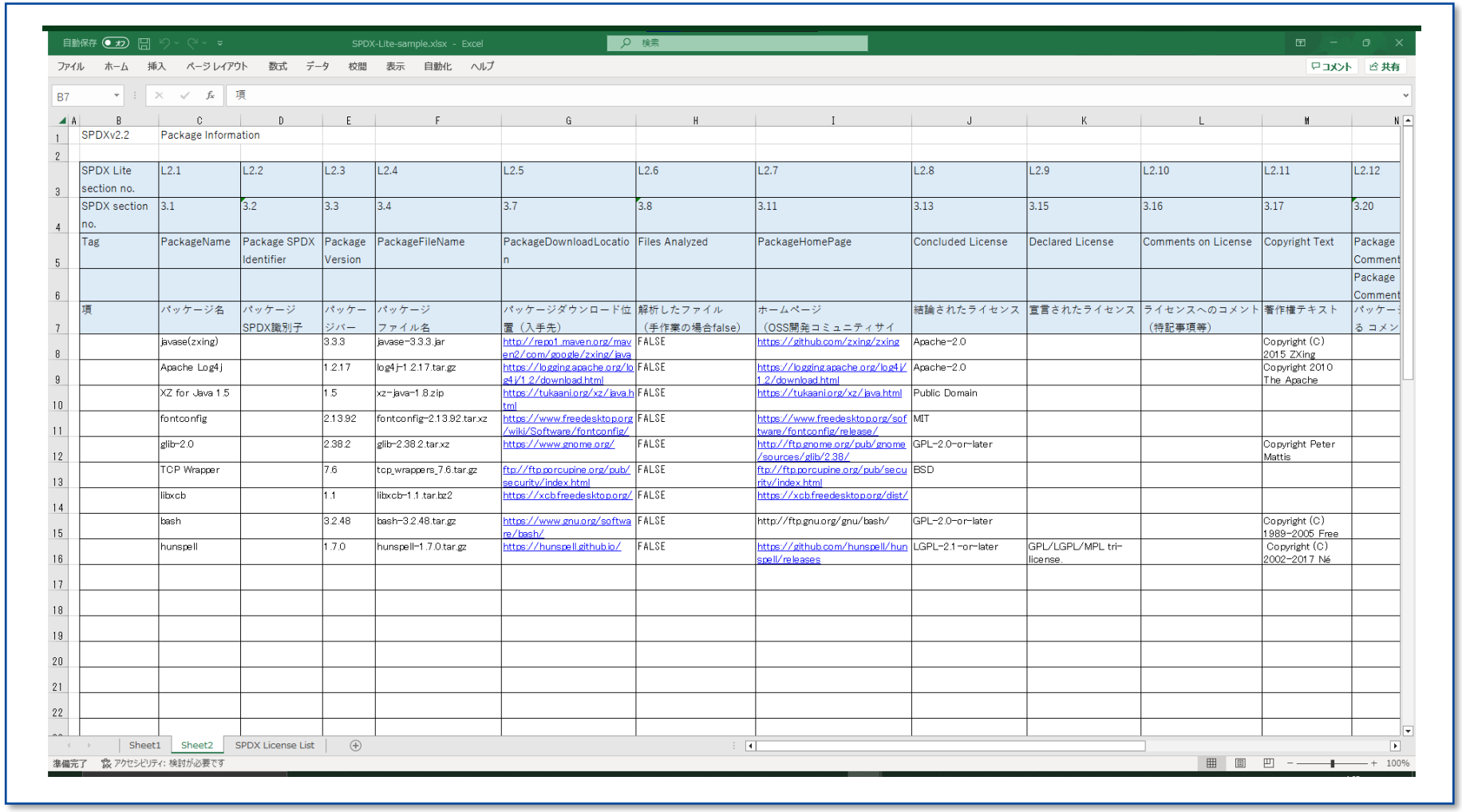
Package-centric

#	SPDX subclause	Field name
L1.1	6.1	SPDX Version
L1.2	6.2	Data License
L1.3	6.3	SPDX Identifier
L1.4	6.4	Document Name
L1.5	6.5	SPDX Document Namespace
L1.6	6.8	Creator
L1.7	6.9	Created
L2.1	7.1	Package Name
L2.2	7.2	Package SPDX Identifier
L2.3	7.3	Package Version
L2.4	7.4	Package File Name
L2.5	7.5	Package Supplier
L2.6	7.7	Package Download Location

#	SPDX subclause	Field name
L2.7	7.8	Files Analyzed
L2.8	7.11	Package Home Page
L2.9	7.13	Concluded License
L2.10	7.15	Declared License
L2.11	7.16	Comments on License
L2.12	7.17	Copyright Text
L2.13	7.20	Package Comment
L3.1	10.1	License Identifier
L3.2	10.2	Extracted Text
L3.3	10.3	License Name
L3.4	10.5	License Comment

SPDX Lite (Annex G of SPDX v2.x) (cont.)

- 非エンジニアがスプレッドシートでSBOMを管理/編集できる



SPDX-Lite-sample.xlsx - Excel

	B	C	D	E	F	G	H	I	J	K	L	M	N
1	SPDXv2.2	Package Information											
2													
3	SPDX Lite section no.	L2.1	L2.2	L2.3	L2.4	L2.5	L2.6	L2.7	L2.8	L2.9	L2.10	L2.11	L2.12
4	SPDX section no.	3.1	3.2	3.3	3.4	3.7	3.8	3.11	3.13	3.15	3.16	3.17	3.20
5	Tag	PackageName	Package SPDX Identifier	Package Version	PackageFileName	PackageDownloadLocation	Files Analyzed	PackageHomePage	Concluded License	Declared License	Comments on License	Copyright Text	Package Comment
6													Package Comment
7	項	パッケージ名	パッケージSPDX識別子	パッケージバー	パッケージファイル名	パッケージダウンロード位置（入手先）	解析したファイル（手作業の場合false）	ホームページ（OSS開発コミュニティサイ	結論されたライセンス	宣言されたライセンス	ライセンスへのコメント（特記事項等）	著作権テキスト	パッケージる コメン
8		javase(zxing)		3.3.3	javase-3.3.3.jar	http://repo1.maven.org/maven2/com/google/zxing/java	FALSE	https://github.com/zxing/zxing	Apache-2.0			Copyright (C) 2015 ZXing	
9		Apache Log4j		1.2.17	log4j-1.2.17.tar.gz	https://logging.apache.org/log4j/1.2/download.html	FALSE	https://logging.apache.org/log4j/1.2/download.html	Apache-2.0			Copyright 2010 The Apache	
10		XZ for Java 1.5		1.5	xz-java-1.8.zip	https://tukaani.org/xz/java.html	FALSE	https://tukaani.org/xz/java.html	Public Domain				
11		fontconfig		2.13.92	fontconfig-2.13.92.tar.xz	https://www.freedesktop.org/wiki/Software/fontconfig/	FALSE	https://www.freedesktop.org/software/fontconfig/release/	MIT				
12		glib-2.0		2.38.2	glib-2.38.2.tar.xz	https://www.gnome.org/	FALSE	http://ftp.gnome.org/pub/gnome/sources/glib/2.38/	GPL-2.0-or-later			Copyright Peter Mattis	
13		TCP Wrapper		7.6	tcp_wrappers_7.6.tar.gz	ftp://ftp.porcupine.org/pub/security/index.html	FALSE	ftp://ftp.porcupine.org/pub/security/index.html	BSD				
14		libxcb		1.1	libxcb-1.1.tar.bz2	https://xcb.freedesktop.org/	FALSE	https://xcb.freedesktop.org/dist/					
15		bash		3.2.48	bash-3.2.48.tar.gz	https://www.gnu.org/software/bash/	FALSE	http://ftp.gnu.org/gnu/bash/	GPL-2.0-or-later			Copyright (C) 1989-2005 Free	
16		hunspell		1.7.0	hunspell-1.7.0.tar.gz	https://hunspell.github.io/	FALSE	https://github.com/hunspell/hunspell/releases	LGPL-2.1-or-later	GPL/LGPL/MPL tri-license.		Copyright (C) 2002-2017 Né	
17													
18													
19													
20													
21													
22													

※ SPDX Lite に沿った記載例から一部抜粋

SBOM に関するガイド

- 各国法規制の動きに対応するように、様々な組織から公開されてくる可能性がある
- 関係するサプライチェーンでの動向を把握しておくことが重要

Bundesamt für Sicherheit in der Informationstechnik (BSI).
“SBOM-Anforderungen: TR-03183-2 stärkt Sicherheit in der Software-Lieferkette“

- https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/TR-03183-2-SBOM-Anforderungen.html
- https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03183/BSI-TR-03183-2.pdf?__blob=publicationFile&v=3
- CRA に対応するSBOMガイドとなることを目的として公開
- データフォーマット：SPDX v2.3 以降、又は、CycloneDX v1.4以降
- 電子署名：言及無し？

Telco-WG, OpenChain Project.
“Draft Proposal for an OpenChain Telco SBOM Specification Version 1.0“

- https://github.com/OpenChain-Project/Telco-WG
- https://github.com/OpenChain-Project/Telco-WG/blob/main/OpenChain%20Telco%20SBOM%20Specification.md
- テレコム業界向けに、テレコムオペレータとテレコムベンダーらが検討しているもの
- データフォーマット：ISO/IEC 5962:2021 (SPDX v2.2.1)
- 電子署名：推奨

※ 現在、Telco-WG と SBOM-SG (Japan-WG) は次の方向で協業を進めている

- 共同で SPDX 3.0 Lite Profile を提案し、現 draft proposal は ガイドライン等として策定する
- 合意に至った理由：特定産業に依らない汎用的な内容のため、より広く普及展開を目指す価値があると考えられた

SBOM に関するガイド (cont.)

- 医療機器などでは個別に規制やガイドラインが整備されている
- IMDRF と FDA は現状ではそれぞれ独立している

FDA (U.S. Food & Drug Administration).
"Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions"

- https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions
- NTIA の Minimum Elements に加えて、医療機器では次の情報を利用者に提供することを推奨する

Information	Description （説明）
Software level of Support	ソフトウェアコンポーネントの製造業者が提供するサポートの水準 Ex. actively maintained (保守提供中), no longer maintained (保守提供終了), abandoned (放棄) ※SPDX V2.x系では対応するデータフィールドがない
End-of-support date	"End of support" 又は "End of life" の期限を明確にする → サポート完了のものであれば、製造業者がセキュリティパッチやソフトウェア更新を提供する合理的な理由があるとは言えなくなる。 → 言い換えれば、サポート期間であれば、製造業者は利用者にサイバーセキュリティリスクについて適切なプロセスを整備して対処する必要がある。 ※ SPDX 2.x系では、ValidUntilDate が相応する

SPDX に基づくデータフィールドの検討例

現行のSPDX仕様 (v2系) では “LifeCycle Phase” と照応するデータフィールドがない

CaseStudy1	Telco-WG proposal draft	SPDX Lite (v2.3)	SPDX Lite (ISO/IEC 5962)	TR-03183-2	NTIA Mnimum Elements
(6.1) SPDX Version	(6.1) SPDX Version	(6.1) SPDX Version	(6.1) SPDX Version		
(6.2) Data License	(6.2) Data License	(6.2) Data License	(6.2) Data License		
(6.3) SPDX Identifier	(6.3) SPDX Identifier	(6.3) SPDX Identifier	(6.3) SPDX Identifier	(6.3) SPDX Identifier	
(6.4) Document Name	(6.4) Document Name	(6.4) Document Name	(6.4) Document Name		
(6.5) SPDX Document Namespace	(6.5) SPDX Document Namespace	(6.5) SPDX Document Namespace	(6.5) SPDX Document Namespace		Other Unique Identifiers
(6.6) External document references					
(6.8) Creator	(6.8) Creator	(6.8) Creator	(6.8) Creator	(6.8) Creator	Author of SBOM Data
(6.9) Created	(6.9) Created	(6.9) Created	(6.9) Created	(6.9) Created	Timestamp
(7.1) Package Name	(7.1) Package Name	(7.1) Package Name	(7.1) Package Name	(7.1) Package Name	Component Name
(7.2) Package SPDX Identifier	(7.2) Package SPDX Identifier	(7.2) Package SPDX Identifier	(7.2) Package SPDX Identifier	(7.2) Package SPDX Identifier	Other Unique Identifiers
(7.3) Package Version	(7.3) Package Version	(7.3) Package Version	(7.3) Package Version	(7.3) Package Version	Version of the Component
(7.4) Package File Name		(7.4) Package File Name	(7.4) Package File Name		
(7.5) Package Supplier	(7.5) Package Supplier	(7.5) Package Supplier		(7.5) Package Supplier	Supplier Name
(7.7) Package Download Location	(7.7) Package Download Location	(7.7) Package Download Location	(7.7) Package Download Location	(7.7) Package Download Location	
	(7.8) Files Analyzed	(7.8) Files Analyzed	(7.8) Files Analyzed		
(7.9) Package verification code					
(7.10) Package Checksum	(7.10) Package Checksum			(7.10) Package Checksum	Component Hash
		(7.11) Package Home Page	(7.11) Package Home Page		
(7.13) Concluded License	(7.13) Concluded License	(7.13) Concluded License	(7.13) Concluded License	(7.13) Concluded License	License Information
(7.15) Declared License	(7.15) Declared License	(7.15) Declared License	(7.15) Declared License	(7.15) Declared License	License Information
(7.16) Comments on License		(7.16) Comments on License	(7.16) Comments on License		License Information
(7.17) Copyright Text	(7.17) Copyright Text	(7.17) Copyright Text	(7.17) Copyright Text		License Information
(7.20) Package Comment		(7.20) Package Comment	(7.20) Package Comment		
(7.21) External Reference field	(7.21) External Reference field	(7.21) External Reference field		(7.21) External Reference field	Other Unique Identifiers
(10.1) License Identifier		(10.1) License Identifier	(10.1) License Identifier		License Information
(10.2) Extracted Text		(10.2) Extracted Text	(10.2) Extracted Text		License Information
(10.3) License Name		(10.3) License Name	(10.3) License Name		License Information
(10.5) License Comment		(10.5) License Comment	(10.5) License Comment		License Information
(11.1) Relationship	(11.1) Relationship			(11.1) Relationship	Dependency Relationship
TBD					Lifecycle Phase
					Other Component Relationships

bg:w hite	Required
bg:green	Conditional
bg:blue	Unclear
bg:purple	TBD
bg:red	NTIA requiement
bg:orange	NTIA reccomendation (*Assuming "Concluded Licednse" is needed)
bg:yellow	NTIA reccomendation (*Including those assumed conditional)

SBOMの作成、管理、流通で見られる話題

1. 誰かがフォークしたソースを使うかどうかは、よく確認して
   - 例：名称もバージョンも同じだけど、ソースコードを弄っていて第三者のコードが混入している場合

2. 内製のコードは可能な限りパッケージ管理のお作法にしたがう
   - C/C++ はたった一つの冴えたパッケージ管理手法では対応できない場合がある。
     conan のみ、conan + 何か、何かのみ、何かの組合せ、などビルド環境の事情に応じて有効な手段を導入すべき。

3. ソースコードスキャンツールを使うときは、ソースコードとそれ以外のファイルも検査する
   - 例：ライセンスの条文はGPL-2.0+ だが、権利者が条文以外の箇所でGPL-2.0 だと宣言している場合
     → そのソースコードとリンクするファイルはGPL-2.0と両立しなくてはならない

4. SPDX文書のライセンスは、 (6.11) DocumentComment も確認する
   - (6.2) DataLicense は 仕様上 “CC0-1.0” だが、秘密保持の対象とする場合は DocumentComment などに追記すべきという議論がある

5. 自動処理はまだまだ発展途上
   - 技術動向とあわせて市場やコミュニティの動向を適切にキャッチアップし、コンセンサス形成に関わるのがよい

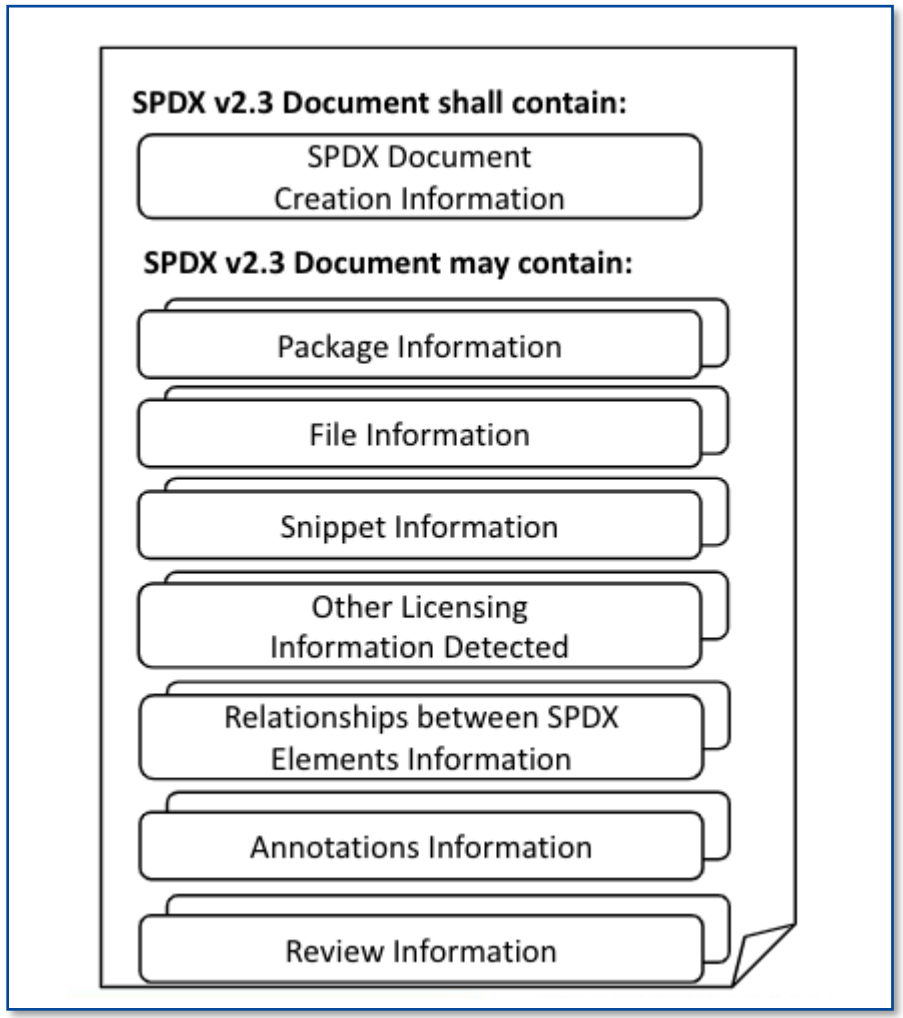
6. 署名について、ただ一つの決まったやり方を強制する動きは今のところみられない
   - 例：Sigstore や GPG を許容する事例が知られている。取引先と要確認。

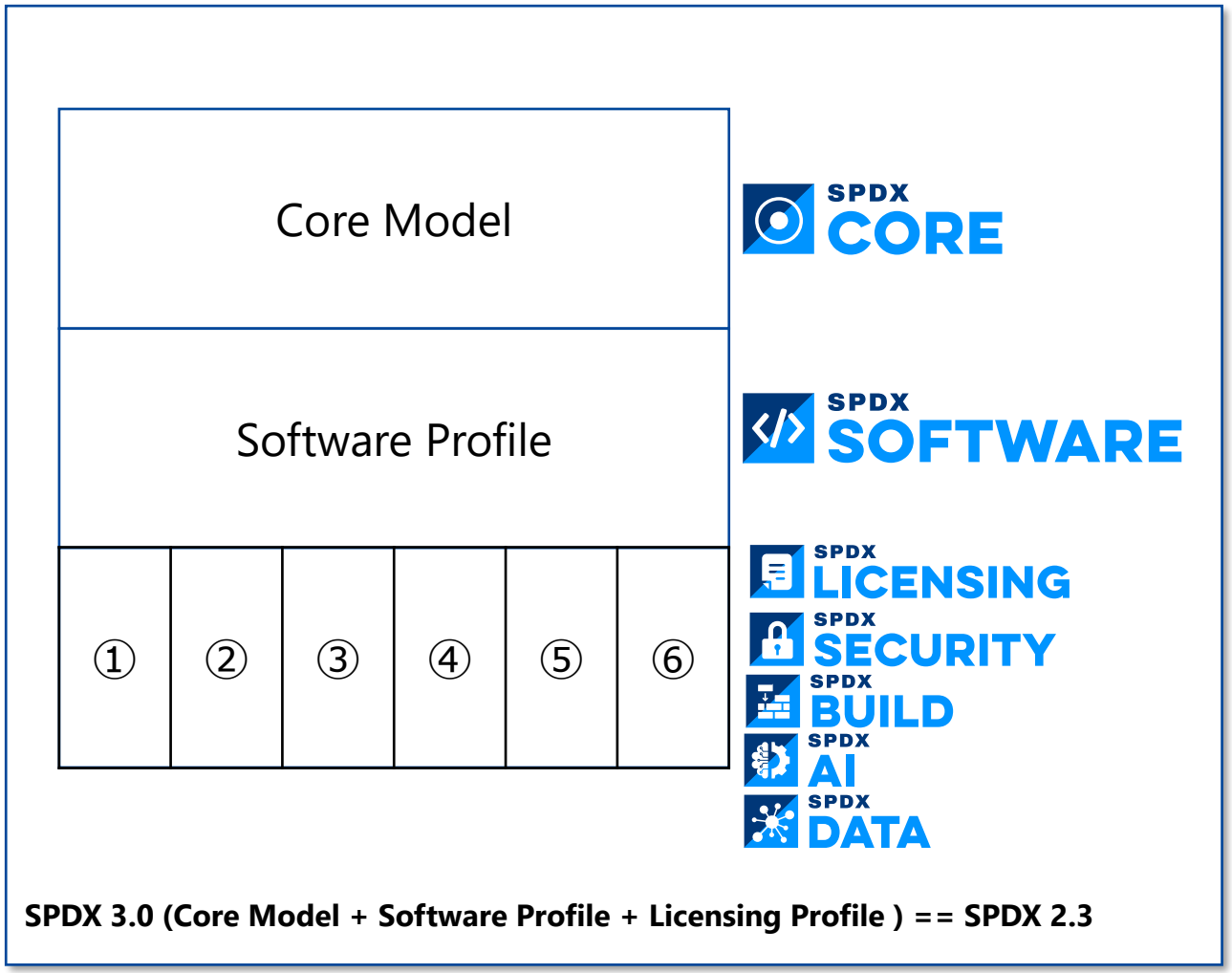
04

SBOM 関連その他の話題

SPDX 2.x -> 3.0

現在、SPDX 3.0 の仕様策定が進む





Software Package Data Exchange (SPDX). https://spdx.dev/

※ Lite も 12月にはロゴができて並ぶはず

SPDX 3.0 (策定中)

クラス、プロパティ、プロファイルを導入し、多様な用途に適用できる拡張性の高い設計を目指す

- Interest in SPDX for additional scenarios and use cases
  - Supporting security and safety critical application compliance requirements
  - AI/ML **and** datasets increasing need for transparency
  - Software Build provenance
- Simplify
  - Profiles
  - Remove confusing names
  - Reorganize and enable general SBOM use cases with minimum overhead
- Flexibility
  - Designed for online access
  - Can communicate a single element
  - Support optional inclusion properties for specific profiles
  - Enhanced relationship structure

SPDX Workgroup. “SPDX Mini Summit”.
Open Source Summit Europe 2023. から
https://www.youtube.com/watch?v=ZCNy9Zsq8b4

SPDX 3.0 (策定中)(cont.)

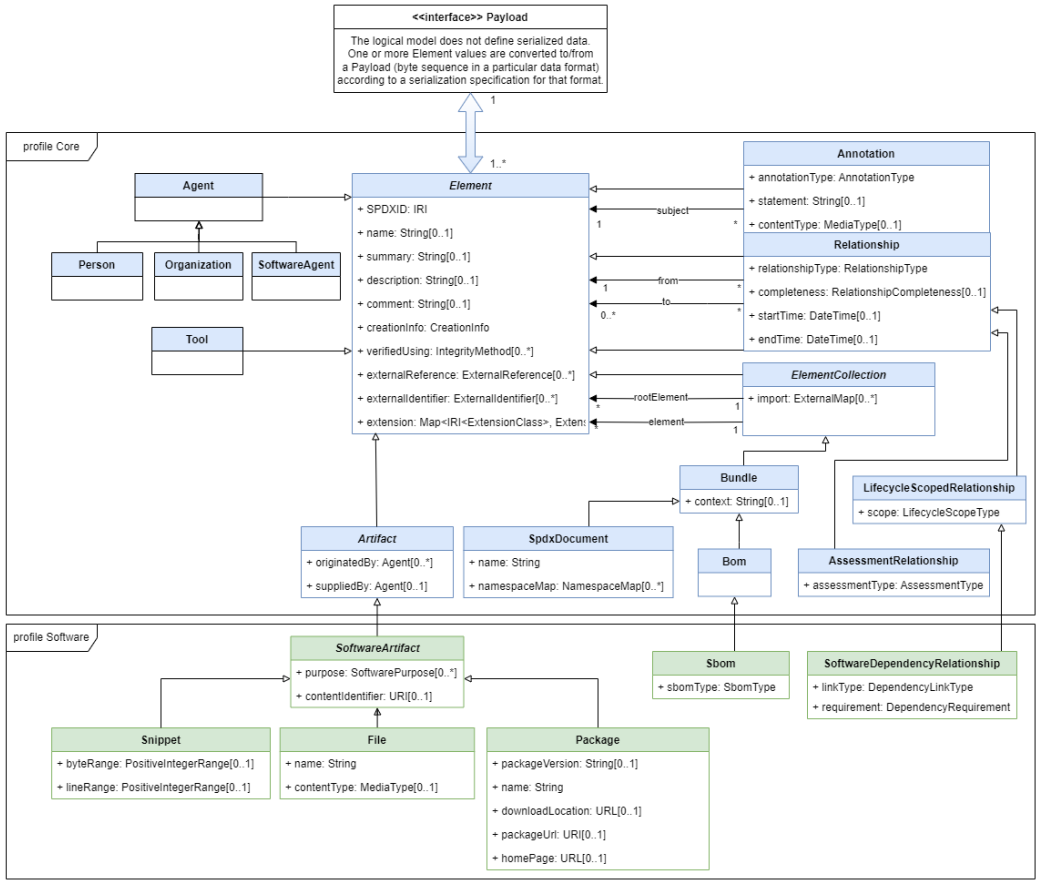
クラス、プロパティ、プロファイルを導入し、多様な用途に適用できる拡張性の高い設計を目指す

- Specification is being transformed into markdown describing
  - Classes, Properties, Enumerations
  - Metadata (type and cardinality) and description for each element
  - Will be able to automatically generate schema from this version (for JSON, YAML, RDF, XML, tag-value, etc) and reduce errors
- Profiles can add their own Classes and Properties and may also restrict other profiles (e.g. values, cardinalities, etc)
- See https://github.com/spdx/spdx-3-model

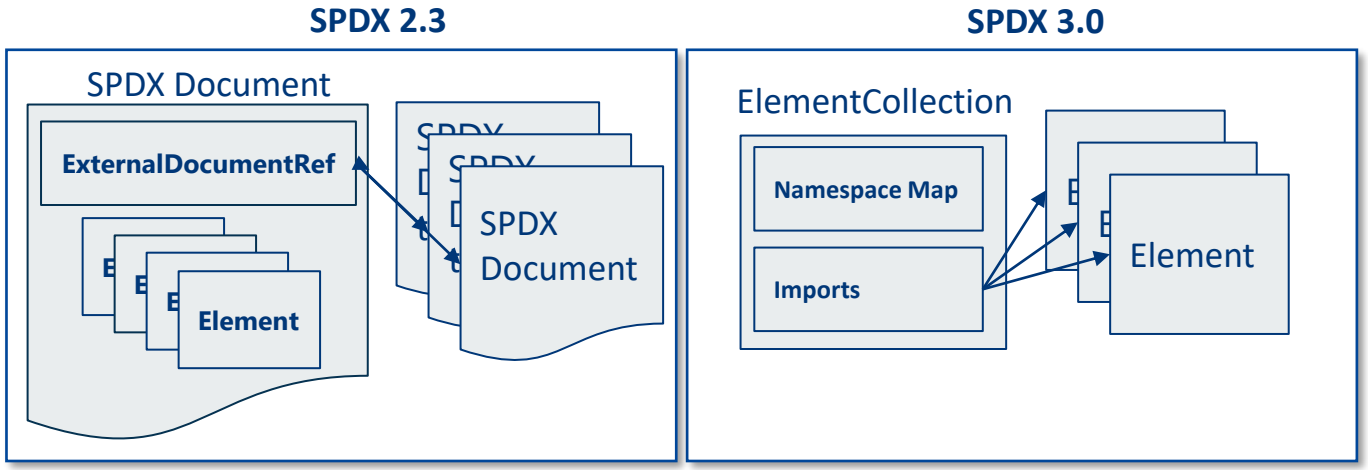
SPDX Workgroup. “SPDX Mini Summit”.
Open Source Summit Europe 2023. から

SPDX 3.0 (策定中)(cont.)

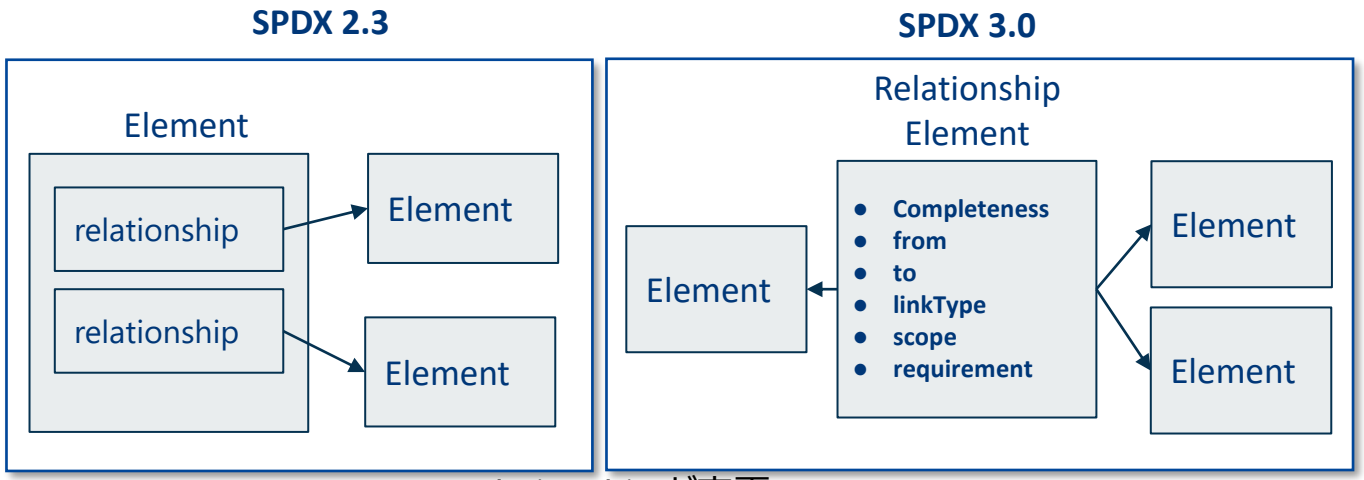
Elementはコレクションでき、Element間を “Relationship” element で関係づける構成に



SPDX Workgroup. “SPDX Mini Summit”.
Open Source Summit Europe 2023. に基づいて作成



External Document Reference が変更



Relationship が変更

SPDX AI Profile properties

Properties borrowed from other profiles

- suppliedBy
- downloadLocation
- packageVersion
- primaryPurpose
- releaseTime

Transparency

Auditability

Traceability

Properties specific to AI profile

- energyConsumption
- standardCompliance
- limitation
- typeOfModel
- informationAboutTraining
- informationAboutApplication
- hyperparameter
- modelDataPreprocessing
- modelExplainability
- sensitivePersonalInformation
- metricDecisionThreshold
- metric
- domain
- autonomyType
- safetyRiskAssessment

SPDX Workgroup. “SPDX Mini Summit”.
Open Source Summit Europe 2023. に基づいて作成

SPDX DATA Profile properties

Properties borrowed from other profiles

- originatedBy
- downloadLocation
- builtTime
- primaryPurpose
- releaseTime

Transparency

Auditability

Traceability

Properties specific to Dataset profile

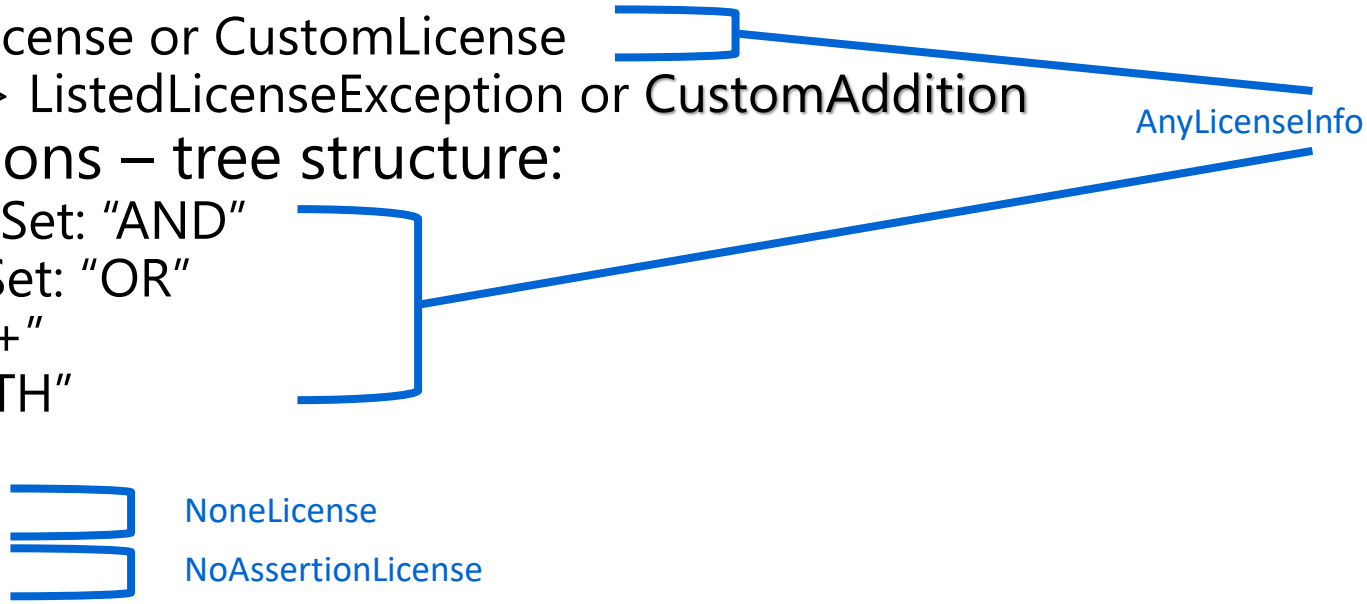
- datasetType
- datasetCollectionProcess
- intendedUse
- datasetSize
- datasetNoise
- datasetSize
- dataPreprocessing
- sensor
- knownBias
- sensitivePersonalInformation
- anonymizationMethodUsed
- confidentialityLevel
- datasetUpdateMechanism
- datasetAvailability

SPDX Workgroup. “SPDX Mini Summit”.
Open Source Summit Europe 2023. に基づいて作成

SPDX Licensing Profile

SPDX LICENSING

- Primary – tree leaves:
  - License => ListedLicense or CustomLicense
  - LicenseAddition => ListedLicenseException or CustomAddition
- Complex combinations – tree structure:
  - ConjunctiveLicenseSet: “AND”
  - DisjunctiveLicenseSet: “OR”
  - OrLaterOperator: “+”
  - WithOperator: “WITH”
- Other values:
  - NONE
  - NOASSERTION

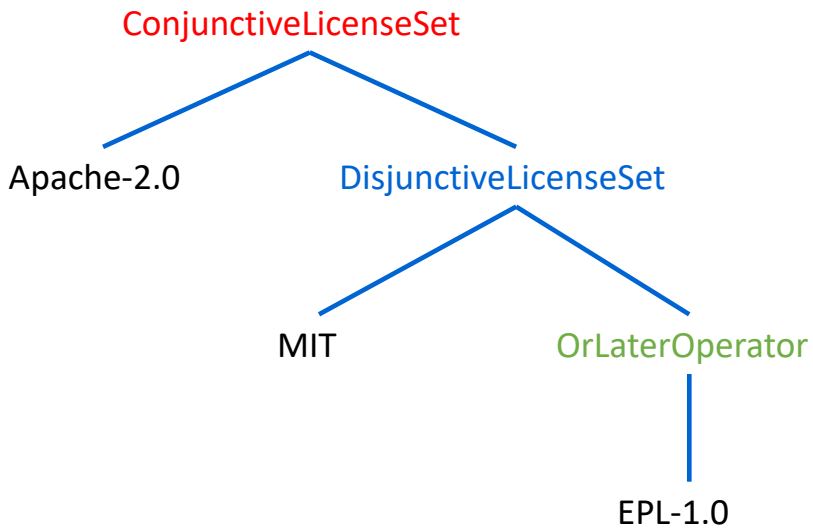


SPDX Workgroup. “SPDX Mini Summit”.
Open Source Summit Europe 2023. に基づいて作成

SPDX Licensing Profile (cont.)

Expression: Apache-2.0 AND (MIT OR EPL-1.0+)

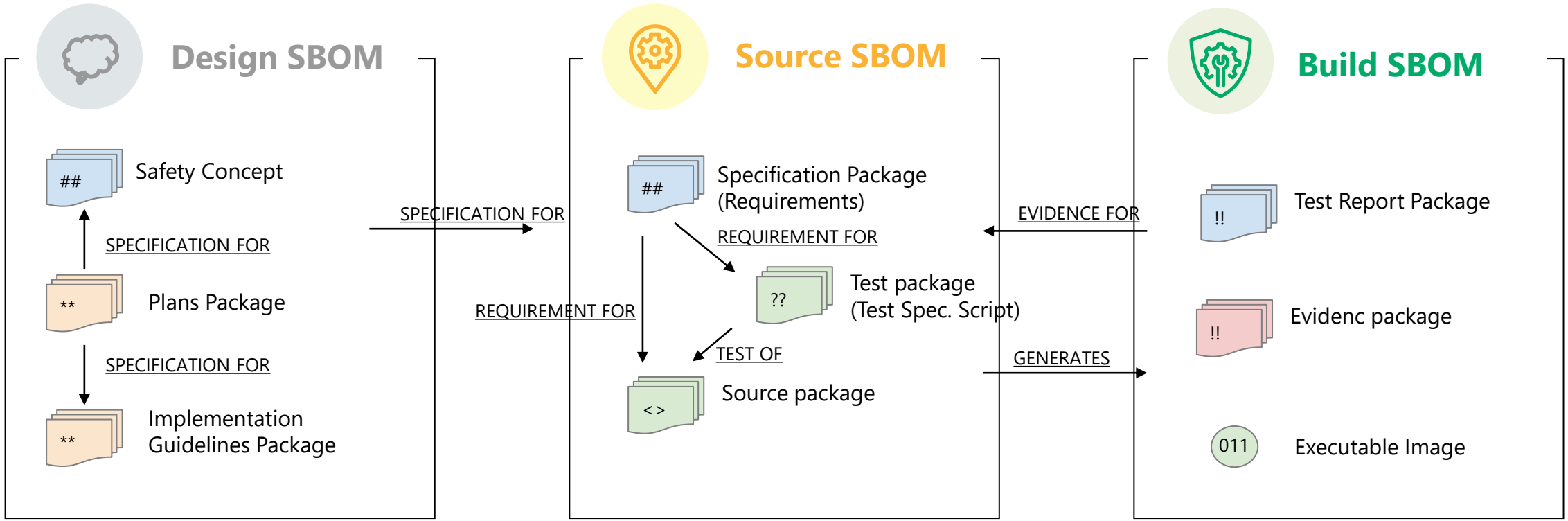
Model:



SPDX Workgroup. “SPDX Mini Summit”.
Open Source Summit Europe 2023. に基づいて作成

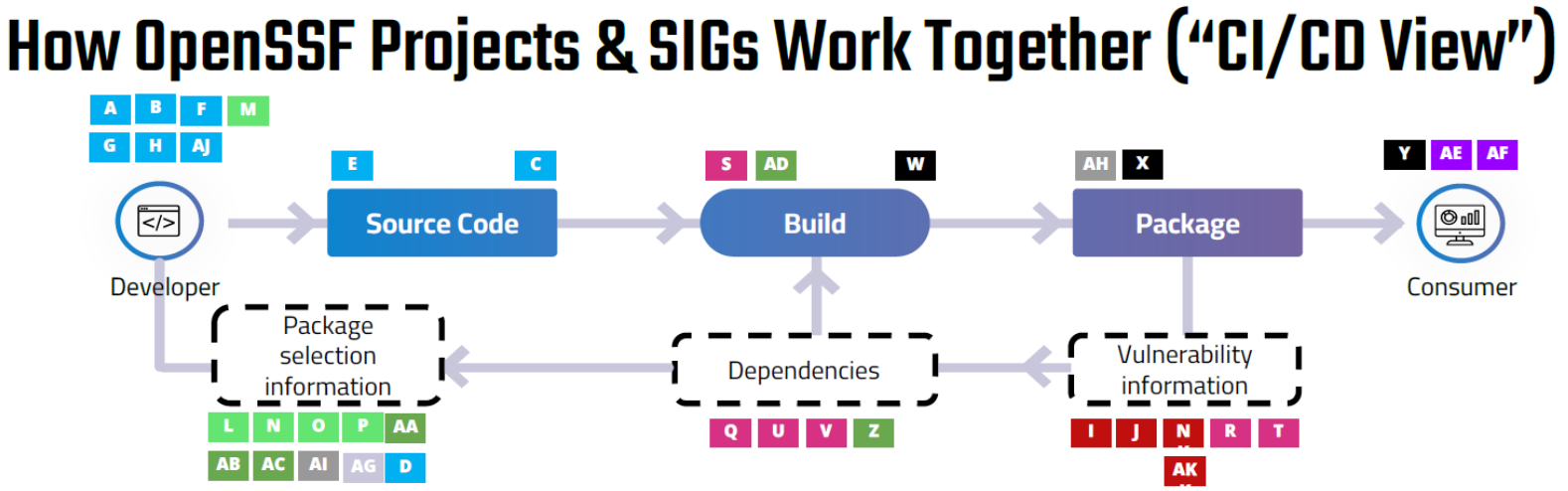
SPDX 3.1 以降か：Functional Safety

SBOM に仕様書やテストを関連付ける



SPDX Workgroup. “SPDX Mini Summit”.
Open Source Summit Europe 2023. に基づいて作成

OpenSSF (Open Source Software Security Foundation) のとりくみ



Best Practices WG

A. **Secure Software Development Fundamentals courses** SIG
B. **Security Knowledge Framework (SKF)** project
C. **OpenSSF Best Practices Badge** project
D. **OpenSSF Scorecard** project
E. **Great MFA distribution SIG**
F. **Common Requirements Enumeration (CRE)** project
G. **Concise & Best Practices Guides** SIGs
H. **Education** SIG - Mob. Plan
AJ. **Memory Safety** SIG - Mob. Plan

Vulnerability Disclosures WG

I. **CVD Guides** SIGs
J. **OSS-SIRT** SIG - Mob. Plan
K. **Open Source Vuln Schema (OSV)** project
AK. **OpenVEX** SIG
AL. **Vuln Autofix** SIG

Identifying Security Threats WG

L. **Alpha & Omega** project
M. **Office Hours** SIG
N. **Security Insights**
O. **Security-Metrics: Risk Dashboard** project - Mob. Plan
P. **Security Reviews** project

Security Tooling WG

Q. **SBOM Everywhere** SIG - Mob. Plan
R. **False-Positive Suppression Spec** SIG
S. *[Guide to Security Tools SIG]*
T. *[cve-benchmark SIG]*
U. **OSS Fuzzing** SIG
V. **DAST scanning & web app**

End Users WG

AE. **Supply Chain Attack taxonomy** SIG
AF. **Supply Chain Attack RefArch** SIG

Supply Chain Integrity WG

W. **Supply-chain Levels for Software Artifacts (SLSA) SIG**
X. **Factory for Repeatable Secure Creation of Artifacts (FRSCA)** SIG
Y. **Secure Supply Chain Consumption Framework (S2C2F)** SIG

Securing Software Repositories WG

AG. **Survey of OSS Repos** SIG

Securing Critical Projects WG

Z. **List of Critical Open Source Projects, components, & Frameworks** SIG
AA. **criticality_score** project
AB. **Harvard study** SIG
AC. **package-feeds / package-analysis** project
AD. **allstar** project

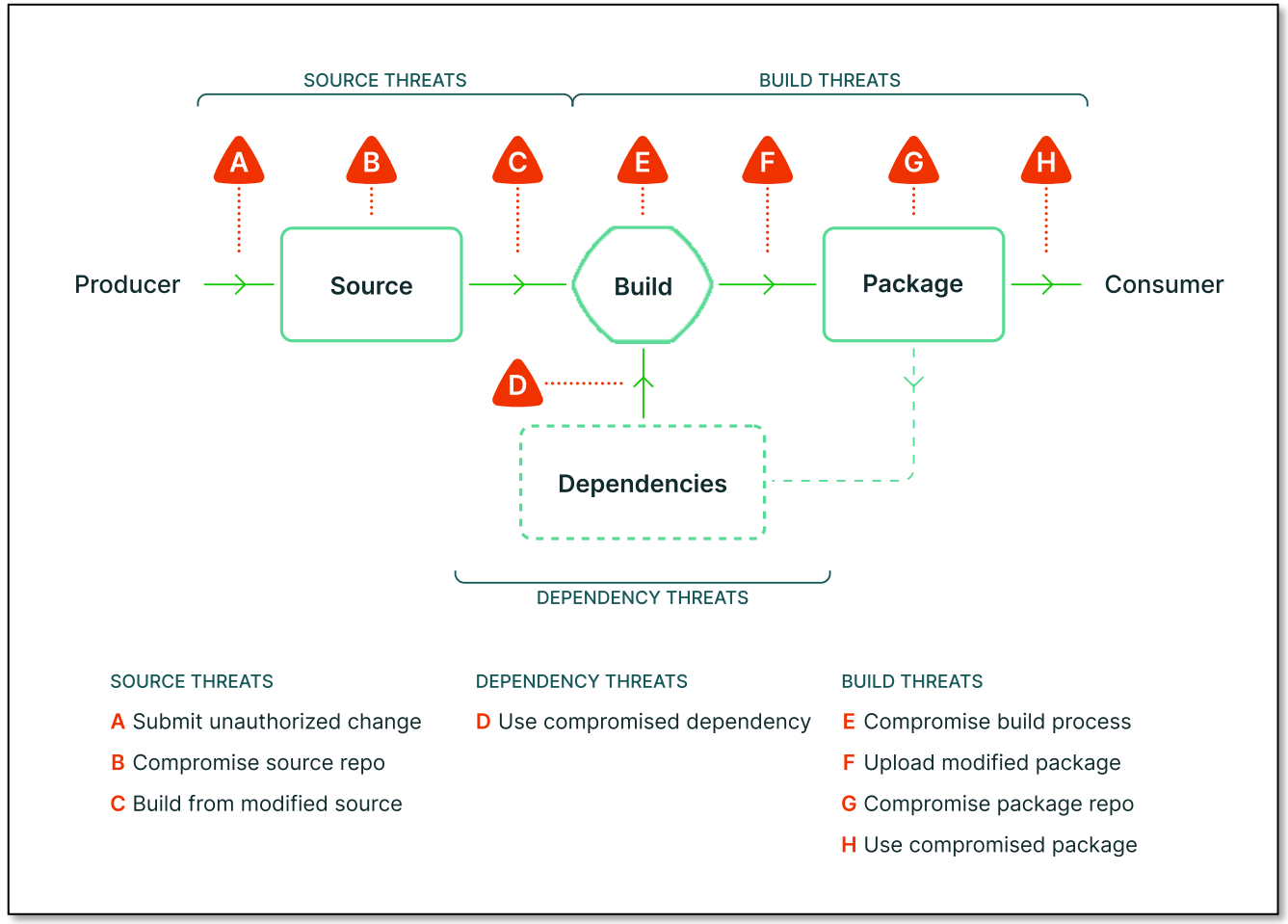
Associated Projects

AH. **sigstore**
AI. **Core Toolchain Infrastructure (CTI) support**

https://openssf.org/community/openssf-working-groups/

SLSA (Supply Chain Levels of Software Artifacts)

ソフトウェアサプライチェーンにおける真正性確保のためのフレームワーク



- ソフトウェアの開発からデプロイに至るまでのプロセスにおいて、「真正性」を確保するため、コンセンサスに基づいて仕様を策定する
- CNCF (Cloud Native Computing Foundation) では傘下プロジェクトにSLSA Assessment を義務付けている*

v1.0仕様は、次のレベルを定義する

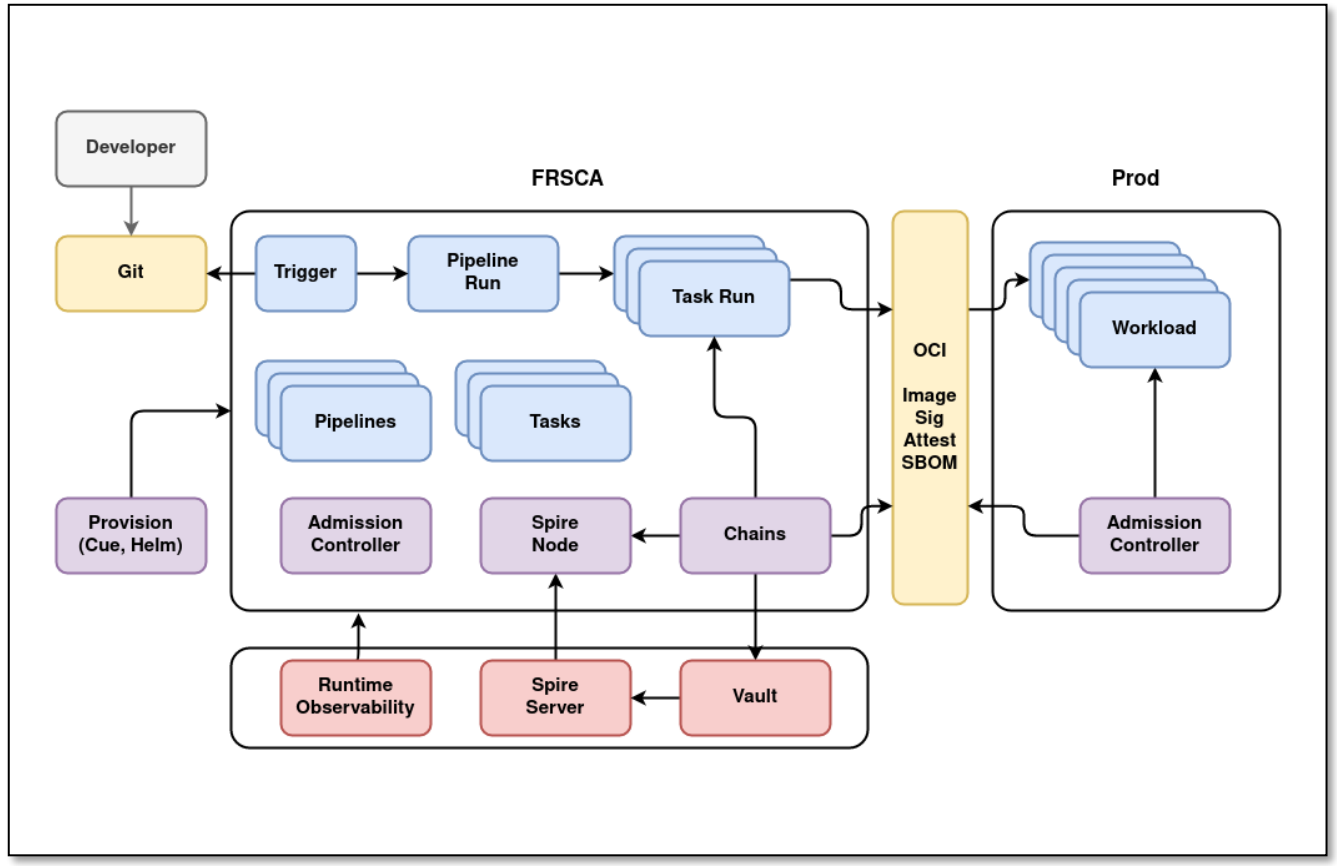
1. パッケージがどのように構築されたかの来歴 (**Provenance**) — 間違い防止
2. ホストされたビルドプラットフォームにより生成された**署名**付きの来歴 — ビルド後の改竄防止
3. 強化された**ビルドプラットフォーム** — ビルド中の改竄防止

https://slsa.dev/

* https://www.cncf.io/blog/2023/04/19/building-secure-software-supply-chains-in-cncf-with-slsa-assessments/

FRSCA (Factory for Repeatable Secure Creation of Artifacts)

セキュアに動作するように構成された、ビルド、パイプライン、署名、可視化、ID、ポリシーのツール群



- すべてのビルドがサプライチェーンセキュリティのベストプラクティスに従うことを保証する、セキュリティガードレールを備えたビルドパイプラインの抽象化と定義のセット

  → いわばリファレンス実装

Kubernetes での利用を前提に次で構成する

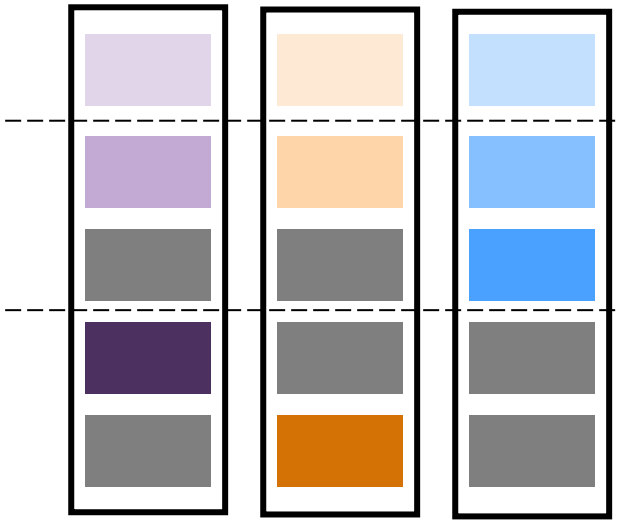
- **CI パイプライン** (Tekton)
- **SBOM生成** (Trivy)
- **AttestationやSBOMへの署名** (sigstore)
- **ワークロードの識別**: SPIFFE準拠 (SPIRE)

https://buildsec.github.io/frsca/

SBOMは、ソフトウェアアセットマネジメントの基礎である

- ソフトウェアリポジトリとCI/CD環境を整備し、利用コンポーネントの一元管理を徹底 (自動化)
- OSSなど部品選定基準を設け、共通性のある機能は「共通基盤」として整備

Before



腕利きまかせ

アプリの開発ラインごとに
部品選定の権限を与えると...

→ 1off モデルのような設計

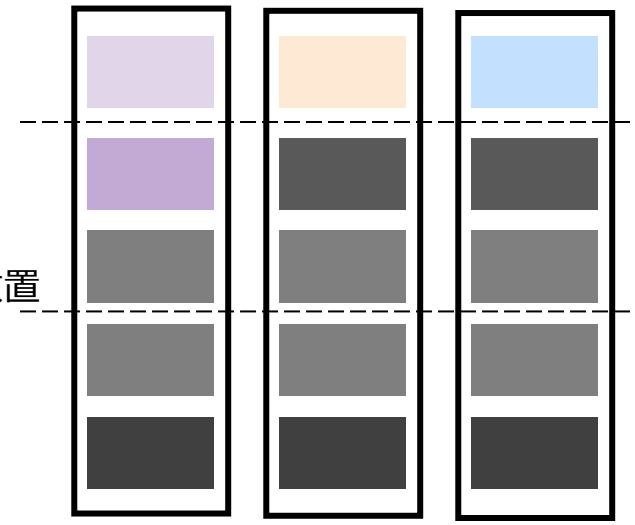
→ 属人的な保守性の悪いコードの放置

→ ライセンスコンプライアンスや
脆弱性管理が煩雑

→ 結果として<u>コスト高</u>

(ソフトウェアにおけるコンポーネントのスタックの例)

After



道具立て

「共通基盤」を整備

→ 独自開発はサービス性に
強く依存する部分に局所化

→ スキル平準化による
動的な人的リソース導入を実現

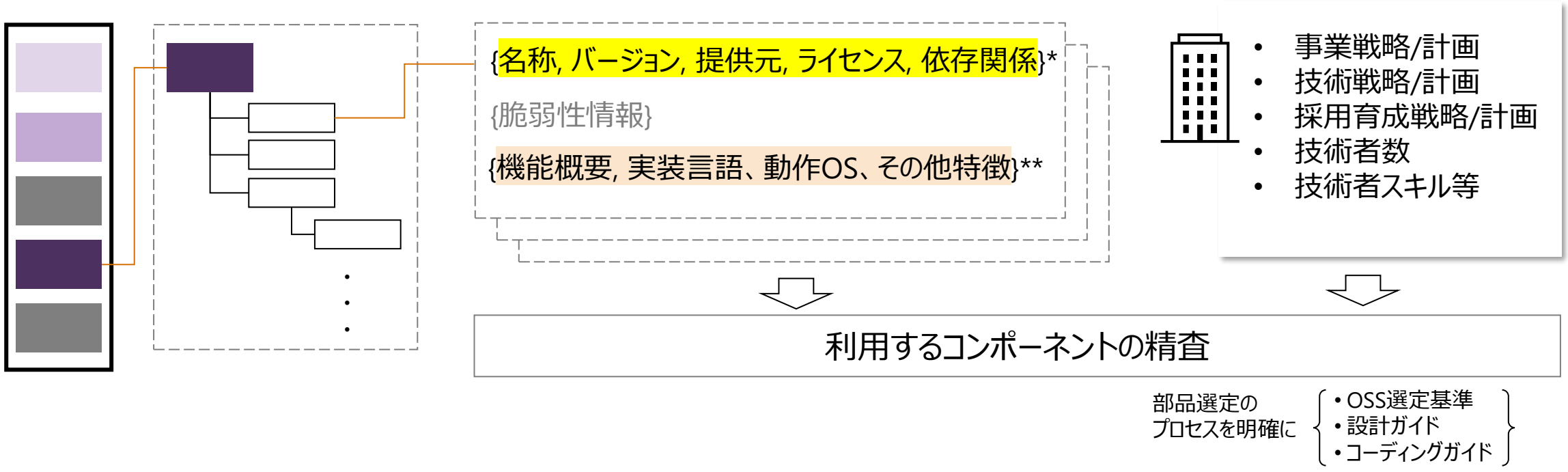
→ リスク管理体制を確立

→ 開発パイプラインの並列化が進み、
迅速なサービスデプロイの実現へ

経営資源である「ソフトウェアアセット」と「ソフトウェア人材」を最大限に活かせるように

SBOMから、自組織のソフトウェア技術(力) を把握する

- ソフトウェアコンポーネントの情報を自動抽出 ＋ 機能などのメタデータを作成
- 自社資源および市場や技術の動向 を整理

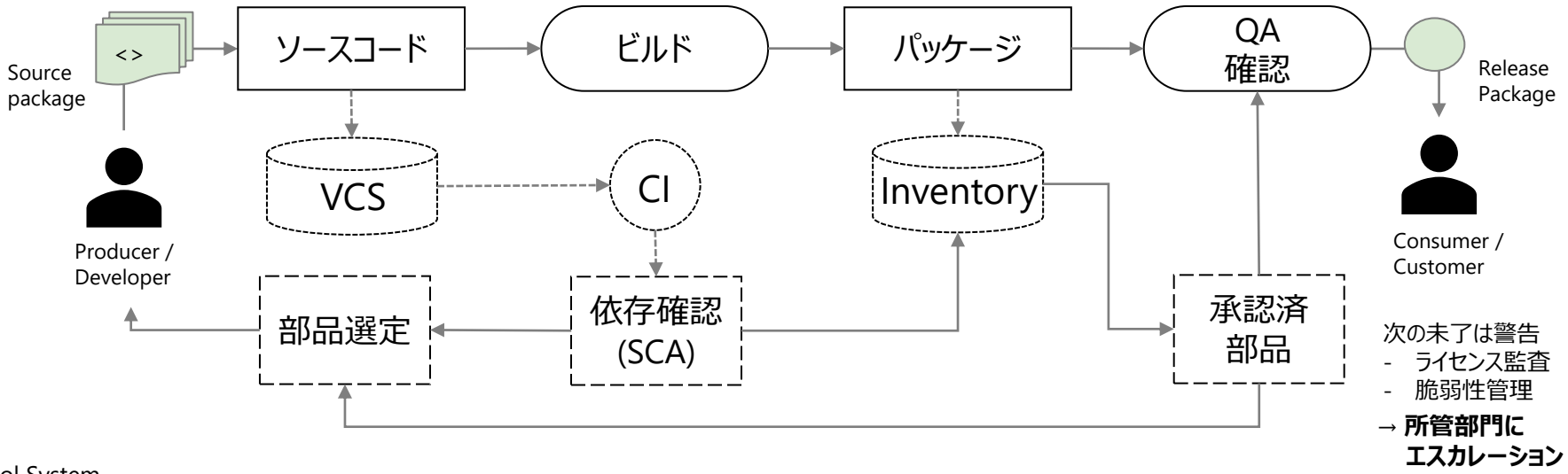


部品選定とスキル平準化で、技術者の生産性と社内流動性を上げる

* SBOMを構成する情報であり、ある程度は自動で生成・管理できる
** 機能概要やその他特徴は、利用実績など評価に基づく情報生成が必要。AI活用による自動化も考えられる

ソフトウェア開発環境の整備

- 「誰が、どのプロジェクトで、どのコードを開発したか」を、VCS で記録管理
- 開発者負担を極力軽減 → 自動化/省力化したワークフローを整備、エスカレーションを自動通知
- ライセンス監査や脆弱性管理が未了のものは警告 → QA通過不可



VCS: Version Control System
CI: Continuous Integration
SCA: Software Composition Analysis
※ 一般的には、SCAに関連して、著作権、ライセンス、脆弱性その他の必要な情報の確認を実施することが知られている

自動化の徹底は負担軽減に加えて、水準の確保、抜け漏れ/恣意的な変更を防止

05

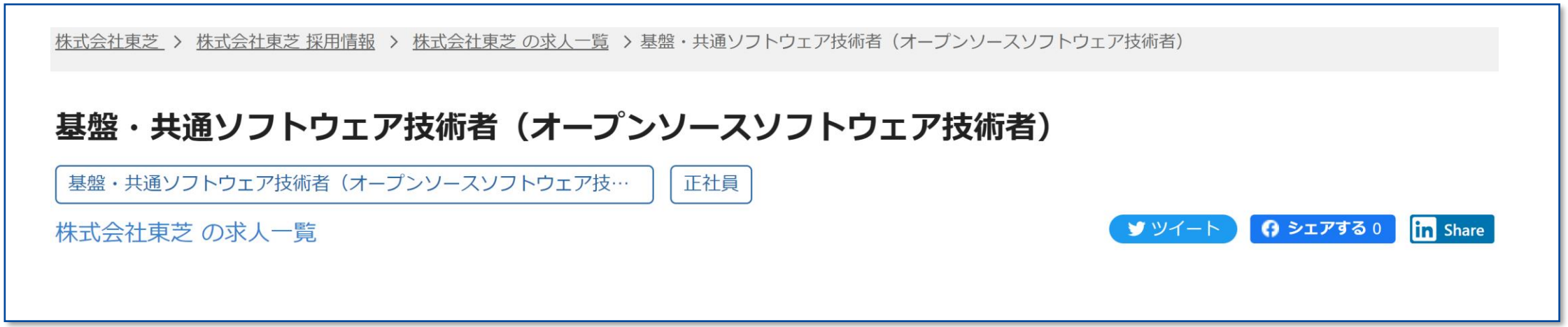
まとめ

まとめ

- リスクマネジメントともいえる、ISO/IEC5230 (オープンソースライセンスコンプライアンス)及び同PRF18974 (セキュリティアシュアランス)のプロセスマネジメントでもSBOMが基礎になっている
- SPDX Lite は、ソフトウェアコンポーネントをパッケージの粒度で管理しようとするものであり、特定産業に依らない汎用的なSBOMデータフォーマットとして利用可能である。
- 次期SPDX 3.0, 3.1 に向けた検討が進んでいる。SPDX 3.0仕様策定に向けたLite Profileの提案の取組も進んでいる。
- セキュリティ観点では、OpenSSFとCNCFなどの取組が盛んである。来歴、アテステーション、署名などCI/CDによるワークフローの自動化が進んでいる。
- SBOMは、リスクマネジメントに留まらず、経営資源としてのソフトウェアアセットマネジメントの基礎にもなる。適切な管理により、オープンソースのエコシステムとともに事業も成長させていくことが重要である。

【求ム】オープンソースソフトウェア技術者

「東芝 オープンソース 求人」で検索か、採用サイトからご覧になれます



仕事内容の例

- データベース、ネットワーク、Web、分散処理、オペレーティングシステムなど共通基盤ソフトウェアの研究開発
- 新規事業の実現に要求される基盤ソフトウェア技術の調査・評価・試作
- 東芝グループの各事業への技術適用
- 社外OSSコミュニティとの連携

「基盤・共通ソフトウェア技術者（オープンソースソフトウェア技術者） | 株式会社東芝」. Retrieved from: https://hrmos.co/pages/toshiba/jobs/0000061

ご清聴頂き、ありがとうございました

Q&A など、意見交換できると幸いです

Takashi Ninjouji

Toshiba Corporation

https://www.linkedin.com/in/takashi-ninjouji/

takashi1.ninjouji@toshiba.co.jp

商標について、その他

- Linux は、Linus Torvalds 氏の日本およびその他の国における登録商標または商標です。
- その他、本ホームページに記載されている社名及び商品名はそれぞれ各社が商標または登録商標として使用している場合があります。
- 本スライドでは、商標「™」、登録商標「®」マークは原則として明記しておりません。
- 本講演資料で取り上げたCivil Infrastructure Platform のオリジナルの紹介資料は次で参照できます。なお、本資料では掲載に当たり一部を変更しています。
  - Urs Gleim. Yoshitake Kobayashi. “Civil Infrastructure Platform : Industrial-Grade Linux” Retrieved from: https://speakerdeck.com/ystk/civil-infrastructure-platform-industrial-grade-linux


TOSHIBA