TOSHIBA

OpenChain Japan-WG 2023年2月会合

オープンソースコンプライアンスのためのプロセスマネジメント標準 ISO/IEC 5230 の適合に向けて

株式会社 東芝
技術企画部　ソフトウェア技術センター　　〇忍頂寺 毅, 白井 保隆, 小山 貴和子
デジタルイノベーションテクノロジーセンター　〇樽家 昌也
技術企画部　技術戦略室　　田村 朱麗

2023.02.09

※本報告は SPI Japan 2022 での同名の報告に基づいており、資料は一部共通です

発表の要旨

ISO/IEC 5230 (OpenChain Specification) に自己認証での適合を達成

5230 仕様要件
1. プログラムの基盤（方針や力量）
2. 関連業務の定義と支援
3. オープンソースコンテンツのレビューと承認
4. コンプライアンス関連資料の作成と頒布
5. オープンソースコミュニティ活動への理解
6. （OpenChainの）仕様要件の遵守

- SPIとOSSの専門家との協業により実現
- その取り組みやノウハウを紹介

発表者：忍頂寺 毅, ソフトウェア技術センター (SWC)

職歴

- 2020.04　東芝入社. オープンソース、インナーソース、SPIの推進
- それ以前　通信事業会社にてR&D, Web/IT企業にて技術管理など

オープンソース関連活動

- Linux Foundation, OpenChain Project (ボードメンバー (東芝))
- Open Invention Network (Technical Advisory Council (東芝))
- SOFTIC OSS委員会 (オブザーバ委員 (東芝))

東芝グループの製品とソフトウェア技術センター

人と、地球の、明日のために。

発表者：樽家 昌也, デジタルイノベーションテクノロジーセンター (DITC)

職歴

- 2019 - DITCのオープンソースプログラムマネージャー,
  DITC HABANEROTS* (BaaS) の開発
- 2018 - DNN-acc, クラウドコンピューティングなどの研究開発
- 2001 - HW/FW/SW 設計実装、Co-design, CAD などの研究開発

オープンソース関連活動

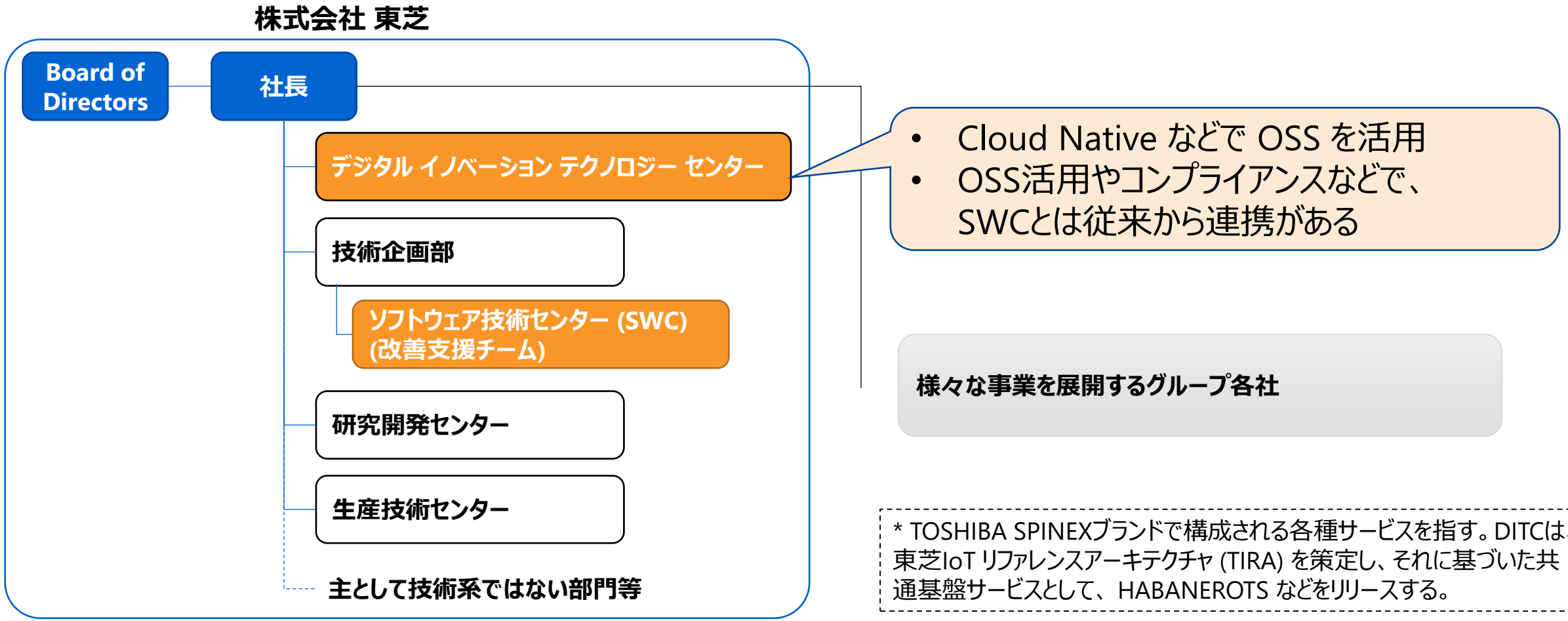
- 2006 - Ruby にコントリビューション
- 2010 - Ruby コアコミッター
  主な関心は、性能改善、タイミングBug など

*HABANEROTS: 東芝IoT (Internet of Things) 基盤サービスとして、IoTシステムの実現に必要な共通機能をクラウド上のWeb APIサービスとして提供する。クラウドネイティブのマイクロサービスで構成しており、Kubernetesなど様々なOSSを活用している。次も参照のこと：
https://www.global.toshiba/content/dam/toshiba/migration/corp/techReviewAssets/tech/review/2020/02/75_02pdf/2-0.pdf

支援対象の組織：デジタルイノベーションテクノロジーセンター (DITC)

ミッション

- B2B As-a-Service ファミリー*の Develop & Deploy



* TOSHIBA SPINEXブランドで構成される各種サービスを指す。DITCは、東芝IoT リファレンスアーキテクチャ (TIRA) を策定し、それに基づいた共通基盤サービスとして、HABANEROTS などをリリースする。

本発表の流れ

01 はじめに

02 ISO/IEC 5230 適合に向けた準備検討

03 ISO/IEC 5230 適合に向けた取り組みの紹介

04 結論

01

はじめに

- OpenChain Specification >> ISO/IEC5230
- ソフトウェアサプライチェーンにおけるリスク管理
- 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 の重要性が高まっている

OpenChain Spec. 2.1 >> ISO/IEC 5230:2020

組織におけるオープンソースを活用するための「プログラム」の要件を定める

OPENCHAIN
(Specification 2.1/2.0)

機能的に同等

TC > ISO/IEC JTC 1
ISO/IEC 5230:2020
Information technology — OpenChain Specification

要件* (*発表者による試訳)
1. プログラムの基盤（方針や力量）
2. 関連業務の定義と支援
3. オープンソースコンテンツのレビューと承認
4. コンプライアンス関連資料の作成と頒布
5. オープンソースコミュニティ活動への理解
6. （OpenChainの）仕様要件の遵守

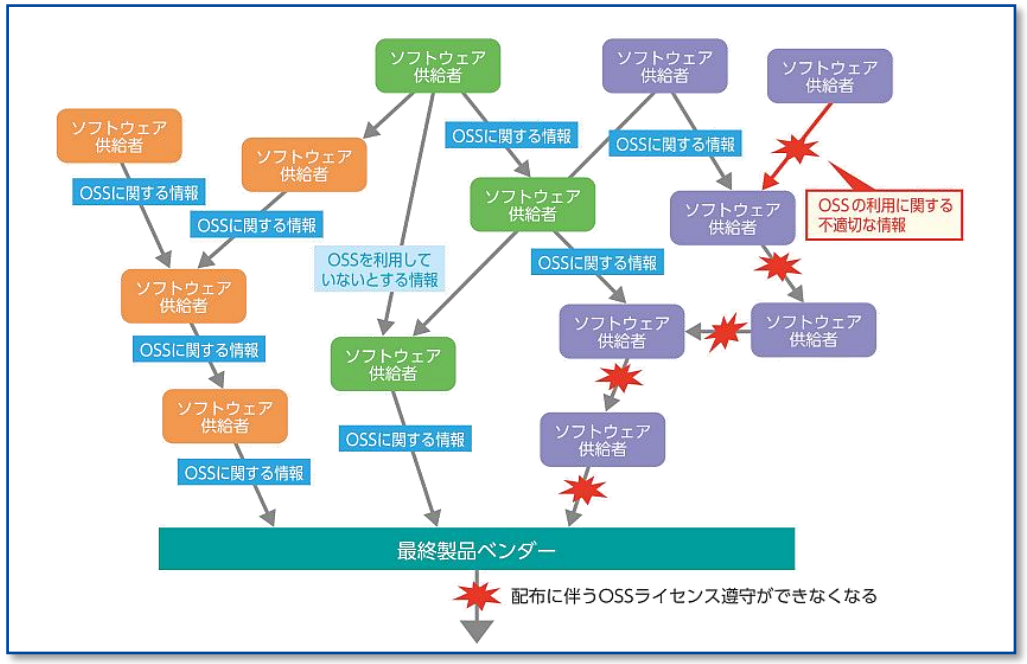
- ✓ Program established
- ✓ Tasks defined
- ✓ Review and approval process
- ✓ Compliance artifacts collected
- ✓ Community engagement policy

オープンソースコンプライアンス標準に基づく
ソフトウェアサプライチェーンにおける「信頼」の構築を図る

出典: OpenChain Project, https://www.openchainproject.org/
ISO/IEC 5230:2020, https://www.iso.org/standard/81039.html?browse=tc

ソフトウェアサプライチェーンにおけるリスク管理

「ラインセンスコンプライアンス」や「脆弱性管理」などがとくに話題になりやすい

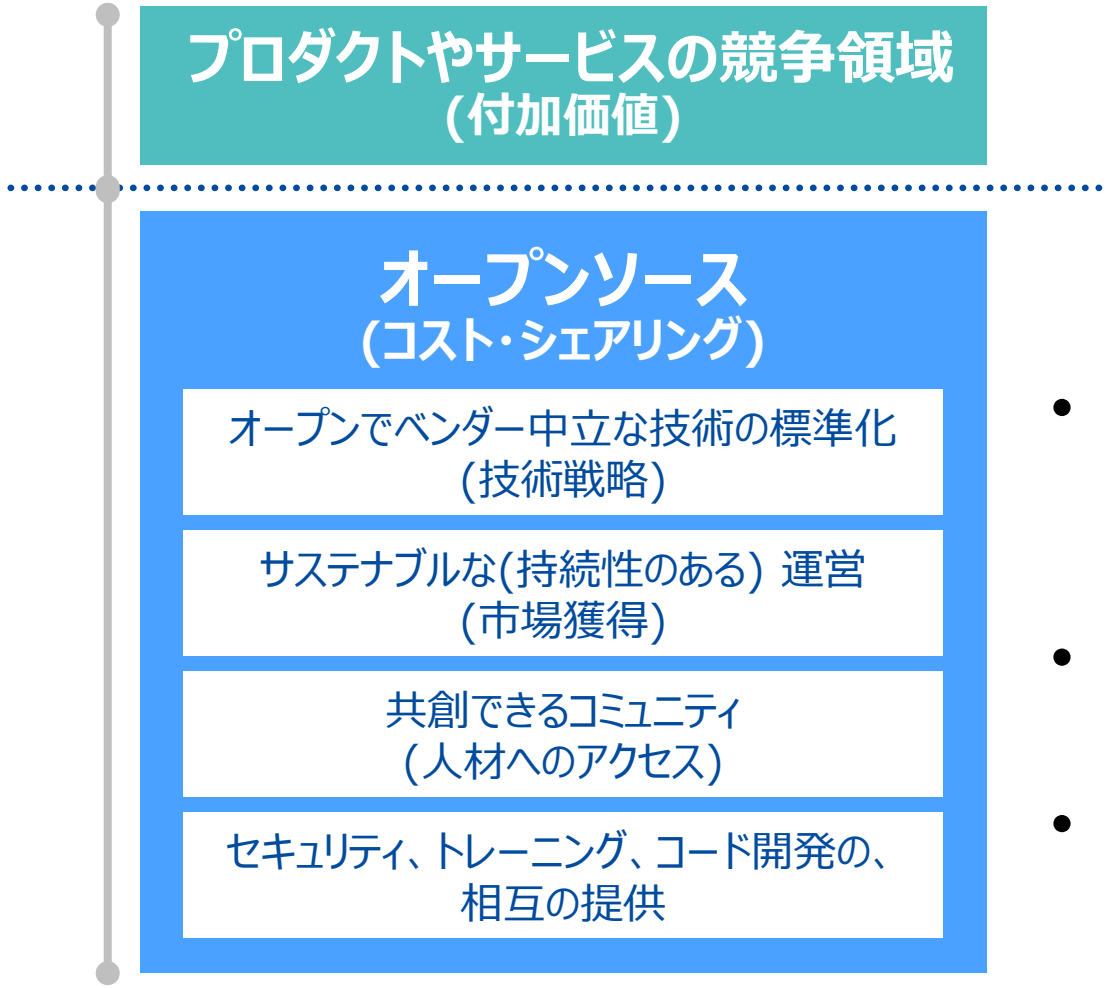


- **ビジネスでのOSS活用が普及拡大**
  - 製品やSDKなどに含まれるOSS
  - OSS自体の大規模化
  - OSSが他のOSSに依存する
- **「どこで、何を」の把握が重要**
  - **SBOM (Software Bill of Materials) による管理運用**の徹底
  - **商流にSBOMも**のせる

※ ISO/IEC 5230 (OpenChain Specification) 適合について、次を評価する指摘が見られる
- プロセス実施とエビデンス管理は、**生産性やリスク予防(リスク予測)の向上**に寄与する
- プロセス実施とエビデンス管理は、OSSを含む**第三者由来のソフトウェアに関するコンプライアンス**に適用できる
- SBOM管理は、**脆弱性管理**の基礎として活用しうる

上図は Japan Work group (the OpenChain Project, Linux Foundation),「オープンソースソフトウェアライセンス遵守に関する一般公衆ガイド」 より

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 の重要性が高まっている



- プロダクトやサービスにおける、
  オープンソースの占める割合は高まりつつある
- ミッションクリティカルなインフラでも同様の傾向
- OSSを含むSBOM管理の整備が必須

東芝グループにおいても、ISO/IEC 5230 の展開が重要

上図は LF Energy High Level Overview Deck（https://www.lfenergy.org/overviewdeck ）などの記載を基に作成

02

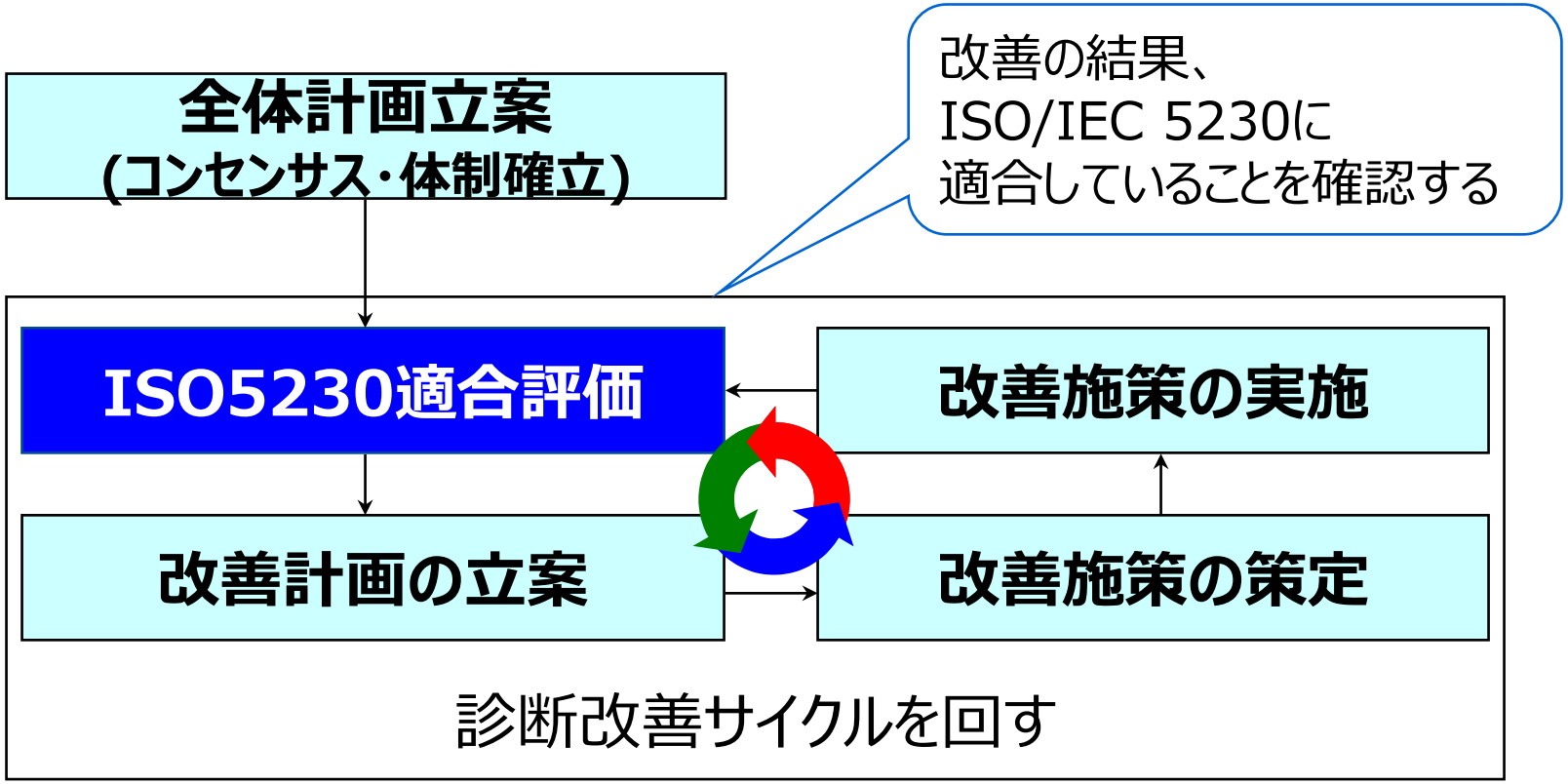
ISO/IEC 5230 適合に向けた準備

- ISO/IEC 5230 適合評価の目的
- ISO/IEC 5230 の要件、その概要、適合条件
- 認証手段： 自己認証 or 第三者認証
- SPI での ISO/IEC 5230 モデルの適用を予備検討
- 適合に向けての方針を策定

SPI での ISO/IEC 5230 モデルの適用を予備検討：ISO/IEC 5230 適合評価の目的

OSS管理の現状を客観的に評価する

- ISO/IEC 5230（OpenChain仕様）を活用し、OSS管理の課題を顕在化させる
- **OSS管理に関する組織の強み、改善の機会を把握**する



ISO/IEC 5230 の要件とその概要：適合するには全項目で○

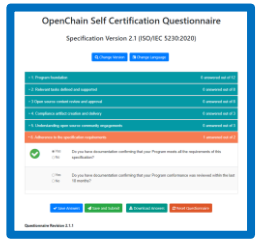
要求項目	概要	評価時
1. OSSコンプライアンスプログラム基盤（方針や力量）	1.1 Policy(ポリシー)組織としてOSS活用やコミュニティ参画への方針が明示されて、周知されている	○
	1.2 Competence(力量) 組織としてOSSを扱う力量管理が行われている	○
	1.3 Awareness(認識) 組織としてプログラムの参加者が十分な認識レベルを維持している	○
	1.4 Program scope(プログラムの適用範囲) 組織としてプログラムのスコープが明確である	○
	1.5 License obligations(ライセンス義務) 組織としてOSSライセンスの履行義務のプロセスが明確である	○
2. 関連業務の定義と支援	2.1 Access(アクセス)組織として第3者からのOSSに関する問い合わせ窓口が明確である	○
	2.2 Effectively resourced(十分なリソース) 組織としてOSSを扱う役割が定義されており、必要なリソースが割り当てられている	○
3. オープンソースコンテンツのレビューと承認	3.1 Bill of Materials(部品表) 組織としてBOMを管理するプロセスがある	○
	3.2 License compliance(ライセンスコンプライアンス) 組織としてOSSライセンスに準拠している	○
4. コンプライアンス関連資料の作成と頒布	4.1 Compliance artifacts(コンプライアンス関連資料) 組織としてライセンスのコンプライアンスに必要な成果物が明確になっていて、管理されている	○
5. オープンソースコミュニティ活動への理解	5.1 Contributions(コントリビューション) 組織としてコミュニティへの貢献を管理する方針と方針を実行するためのプロセスが明示されている。	○
6. （ISO/IEC 5230 の）仕様要件遵守	6.1 Conformance(適合) 組織として ISO/IEC 5230 に適合していることを確認している	○
	6.2 Duration(期間) 組織として、過去18ヶ月以内に、ISO/IEC5230に適合していることを確認している	○

原文は英語。本表は発表者による試訳

認証手段： 自己認証 or 第三者認証

いずれの手段であっても、**「適合」とする扱いは等しい**

自己認証



自己認証のための
質問項目について、
すべて **“YES”** であること

達成水準など “How” は適合を果たそうとする組織が自ら定める必要がある

仕様書、自己認証のための質問項目、オープンソースコミュニティや市場の動向などを踏まえて、**自社での基準策定が重要**

第三者認証

パートナー企業による認定

第三者認証のために統一的な基準はとくにない

【参考】
現時点で、CMMI アプレイザルのような認定資格などはない

出典: 左囲み図 https://certification.openchainproject.org/survey.html?locale=en
右囲み図 https://www.openchainproject.org/partners

認証手段： 自己認証 or 第三者認証 (cont'd)

自己認証の採用事例が多くみられる

Publicly Announced ISO/IEC 5230 Programs

2020/12/01	TOYOTA
2020/12/15	NCSOFT
2020/12/17	Cisco
2021/01/13	NTT Data
2021/02/01	Microsoft
2021/02/08	HITACHI
2021/03/02	LG
2021/04/06	Nanjing Fujitsu Nanda Software Technology Co., Ltd.
2021/04/22	Keitaro
2021/07/07	Samsung Electronics
2021/07/13	Bosch
2021/08/09	Sony Semiconductor
2021/08/19	QCT
2021/08/22	Coontec
2021/09/07	Woven Planet
2021/09/08	Synology
2021/09/08	SK Telecom
2021/10/19	NEC
2021/12/15	ETRI
2022/01/24	Kakaobank
2022/01/24	Kakao
2022/02/14	GBase 8a from General Data Technology Co., Ltd. (GBASE)
2022/02/14	KingbaseES V8 from CETC Kingbase
2022/02/14	Tidb enterprise v4.0 from PingCap
2022/03/17	BlackBerry
2022/03/28	Revenera
2022/03/28	SAP
2022/04/06	TOSHIBA

ハイライトした組織は自己認証による

https://www.openchainproject.org/news を基に作成

SPI での ISO/IEC 5230 モデルの適用を予備検討

ISO/IEC 5230 は、組織のプロセス整備とオープンソースコンプライアンスの複合領域

5230 仕様要件
1. プログラムの基盤（方針や力量）
2. 関連業務の定義と支援
3. オープンソースコンテンツのレビューと承認
4. コンプライアンス関連資料の作成と頒布
5. オープンソースコミュニティ活動への理解
6. （OpenChainの）仕様要件の遵守

診断改善スキル

OSS活用の知見

※矢印は、それぞれの専門家の強みが出やすい例
実際には、個々の事情による

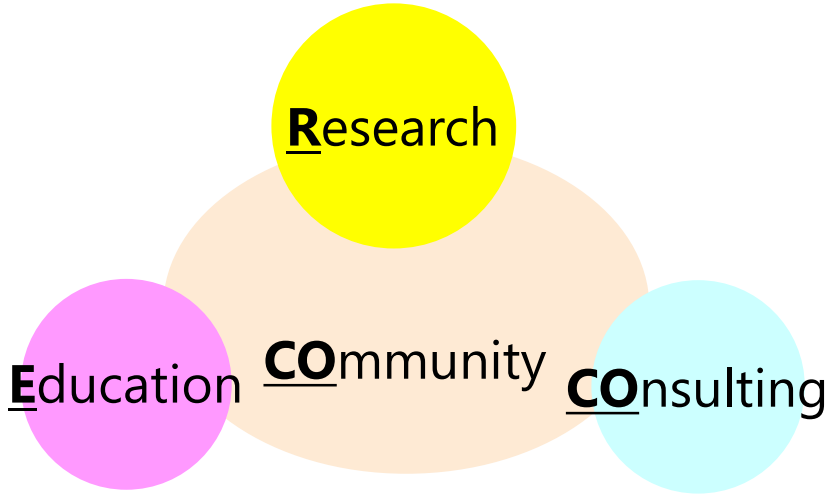
両者がペアになれば、得意分野をいかんなく発揮できる

SPI での ISO/IEC 5230 モデルの適用を予備検討 (cont'd)

前提1：東芝グループにおける、ソフトウェア開発プロセス改善 (SPI) という基盤

- 参照するプロセス標準の例
  CMMI, ITIL 4, ISO/IECs, etc. ← ISO/IEC 5230:2020
- 導入支援するソフトウェア開発手法の例:
  Agile, DevOps, Microservice Architecture (MSA)

前提2：RECOCO モデルによる、社内開発の支援と、東芝グループの連携体制



- R: 研究開発 (改善を推進する技術)
- E: 教育 (人材開発)
- CO : コンサルティング (開発現場でのSPI支援)
- CO : コミュニティ (実践し、それを共有するコミュニティ)

SPI での ISO/IEC 5230 モデルの適用を予備検討：RECOCO への当てはめ

要求項目	概要
1. OSSコンプライアンスプログラム基盤（方針や力量）	1.1 Policy(ポリシー)組織としてOSS活用やコミュニティ参画への方針が明示されて、周知されている
	1.2 Competence(力量) 組織としてOSSを扱う力量管理が行われている
	1.3 Awareness(認識) 組織としてプログラムの参加者が十分な認識レベルを維持している
	1.4 Program scope(プログラムの適用範囲) 組織としてプログラムのスコープが明確である
	1.5 License obligations(ライセンス義務) 組織としてOSSライセンスの履行義務のプロセスが明確である
2. 関連業務の定義と支援	2.1 Access(アクセス)組織として第3者からのOSSに関する問い合わせ窓口が明確である
	2.2 Effectively resourced(十分なリソース) 組織としてOSSを扱う役割が定義されており、必要なリソースが割り当てられている
3. オープンソースコンテンツのレビューと承認	3.1 Bill of Materials(部品表) 組織としてBOMを管理するプロセスがある
	3.2 License compliance(ライセンスコンプライアンス) 組織としてOSSライセンスに準拠している
4. コンプライアンス関連資料の作成と頒布	4.1 Compliance artifacts(コンプライアンス関連資料) 組織としてライセンスのコンプライアンスに必要な成果物が明確になっていて、管理されている
5. オープンソースコミュニティ活動への理解	5.1 Contributions(コントリビューション) 組織としてコミュニティへの貢献を管理する方針と方針を実行するためのプロセスが明示されている。
6. （ISO/IEC 5230 の）仕様要件遵守	6.1 Conformance(適合) 組織として ISO/IEC 5230 に適合していることを確認している
	6.2 Duration(期間) 組織として、過去18ヶ月以内に、ISO/IEC5230に適合していることを確認している

SPI での ISO/IEC 5230 モデルの適用を予備検討：RECOCO への当てはめ (cont'd)

要求項目	概要
1. OSSコンプライアンスプログラム基盤（方針や力量）	1.1 Po 1.2 Co 1.3 Av 1.4 Pr 1.5 Li
2. 関連業務の定義と支援	2.1 Ac 2.2 Ef 組
3. オープンソースコンテンツのレビューと承認	3.1 Bi 3.2 Li
4. コンプライアンス関連資料の作成と頒布	4.1 Co 組
5. オープンソースコミュニティ活動への理解	5.1 Co プロセス
6. （ISO/IEC 5230 の）仕様要件遵守	6.1 Co 6.2 D

SPI が培ってきたRECOCOモデル：

- **R: 研究開発 (改善を推進する技術)**
  ➡ オープンソース関連動向、5230仕様及び適合の解釈や運用など
- **E: 教育 (人材開発)**
  ➡ オープンソースに関する教育素材の開発、など
- **CO：コンサルティング (開発現場でのSPI支援)**
  ➡ 診断、改善
- **CO：コミュニティ (実践し、それを共有するコミュニティ)**
  ➡ 経営層を含む東芝グループ全体での共有と連携

OSS専門家からSPIへの貢献 (上記以外)：

- **開発現場におけるOSS活用実態の把握,**
- **適切なライセンスのポリシーの検討,**
- **コンプライアンス成果物の内容とその管理プロセスの検討, etc**

※ 組織としての診断と改善は、SPI専門家にドライブしてもらうのがよかった

※矢印は、それぞれの専門家の強みが出やすい例。実際には、個々の事情による

適合に向けての方針を策定

採用する認定手段：**自己認証**

既存の資産を有効活用する
- すでにあるルールやプロセスをできるだけ取り込む
- SPIで培った診断と改善のノウハウ

自己認証による適合を通じて、次に掛かるノウハウを得たい
- 自社の**実態の把握**
- 展開における**勘所の検証**

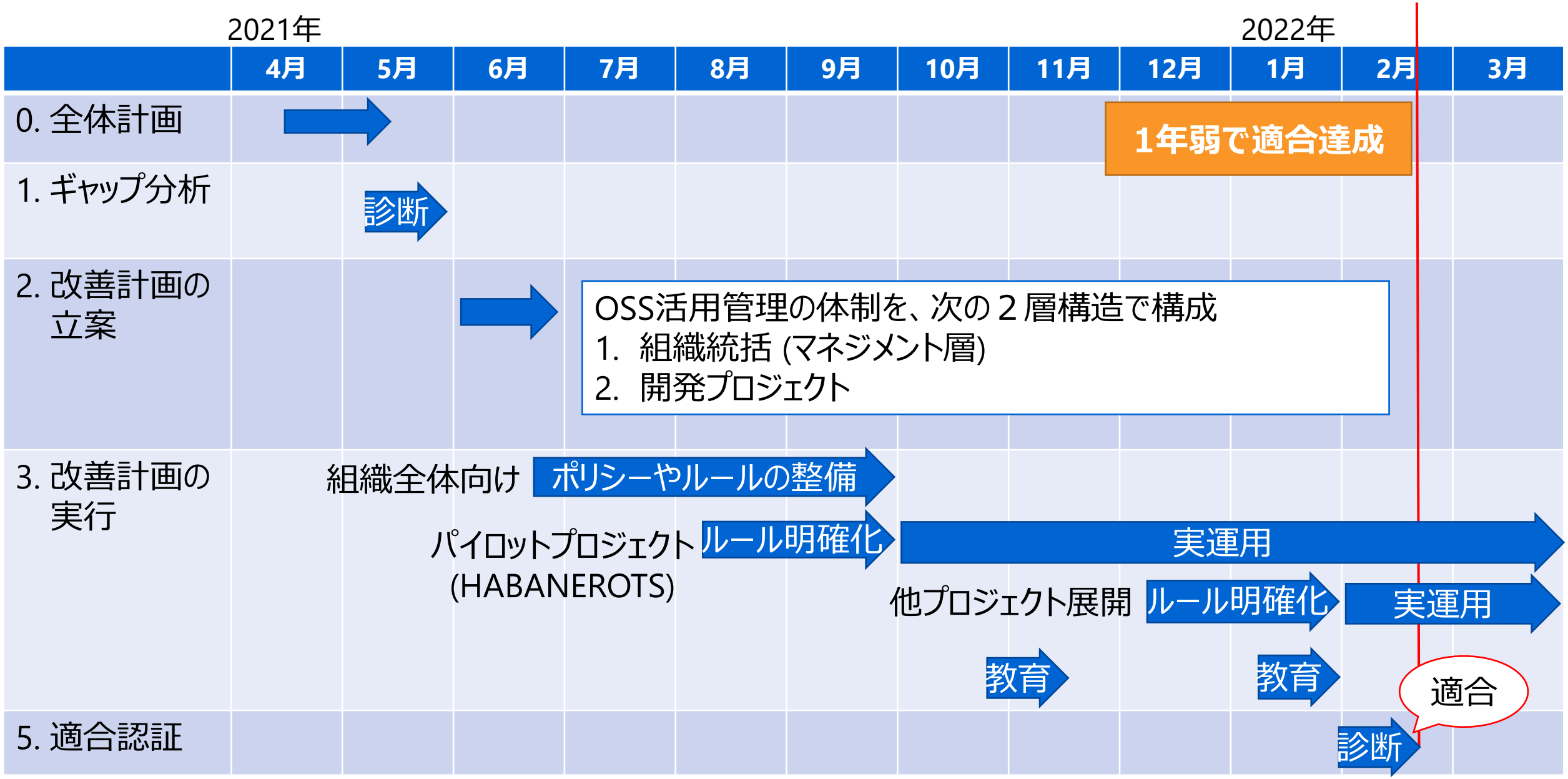
既存の資産の活用により、次のコストを最小化する余地にも期待
- **ポリシー、プロセス、ルールおよび関連する文書の整備**
- **関連する部門との調整**

03

ISO/IEC 5230 適合に向けた取り組みの紹介

- 支援対象の組織
- 5230 適合認証までの道のり
- 5230適合に向けたフォーメーション
- 仕様、質問項目、解釈などの対応づけ
- 自己認証における評価手順および評価基準
- インタビューの進め方
- ギャップ分析 -> 改善 -> 再評価

5230 適合認証までの道のり



5230適合に向けたフォーメーション

業務、プロセス改善、オープンソースを熟知する者をコアメンバーに据える

DITC

プログラムオーナー
(社内でのソフトウェア開発とオープンソースを熟知*) (*Ruby のコアコミッター)

プログラム支援の管理職
(経営幹部含む管理職との調整や承認手続きなど)

×

改善支援チーム

SPI専門家
(プロセス改善の知見を活かして全体管理や部門間調整など)

OSS専門家
(OpenChain仕様やオープンソース動向を熟知)

開発とOSSを知るオーナーのリーダーシップ、管理職による経営層への働きかけ、が、経営層からのエンドースメントに繋がり、大きな原動力を形成

自己認証における評価手順および評価基準

- OpenChain Project が提供する自己認証のための質問項目に基づいて評価
- IOS/IEC 5230 は様々な産業及び事業規模の組織で適用できるようにするため、抽象的な記述が多い → 改善支援チームは仕様策定や普及活動に関与し解釈などのノウハウを収集
- 現在の東芝方式案では、要件について複数の質問項目がある場合、個別の項目ごとに評価したうえで、要件の達成について次とする
  - △が1つでもある：△
  - ×が１つでもある：×

評価	概要
○	• 要求事項を一通り実施している （文書化された手順/プロセスに従って、要求事項を実施している）
△	• 要求事項に相当することが実施されているが、手順は文書化されていない • 要求事項に相当することが実施されているが、担当者の裁量で実施されている
×	• 文書化された手順はあるが、実施されていない • 実施されていない、及び、文書化された手順もない
N/A	• 非該当

仕様、質問項目、解釈などの対応づけ

仕様と質問項目の対照表 を作成

章番号	En	カテゴリ	質問No.	質問項目（En）
3	Requirements	heading		
3.1	Program foundation	heading		
3.1.1	Policy	heading		
3.1.1.0	A written open source policy exists that governs open source license compliance of the supplied software. The policy must be internally communicated.	requirement		
3.1.1.1	A documented open source policy.	verification_material	1.a	Do you have a documented policy that governs open source license compliance of the Supplied Software distribution (e.g., via training, internal wiki, or other practical communication method)?

仕様、質問項目、解釈などの対応づけ (cont'd)

ギャップ分析チェックシートとしても活用

章番号	Ja	カテゴリ	質問No.	概要	質問項目(Ja)	適合の解釈	必要なもの	評価	総合コメント	組織統括	開発部門
3	要求事項	heading									
3.1	プログラムの基盤	heading									
3.1.1	ポリシー	heading									
3.1.1.0	(割愛)	requirement									
3.1.1.1	文書化されたオープンソースポリシー。	verification_material	1.a	対象する組織が従うべき(全社方針に基づいた)OSSプログラムのポリシーがあること	トレーニングや内部wiki、またはその他実用的な通信方法を通しての）供給ソフトウェア配信のオープンソースライセンスコンプライアンスについて規定しているポリシー文書を持っていますか？	文書のように、参照可能な形式で共有される体裁を整えていること。	文書として、「OSSポリシー」、「OSS関連教育資料」、「各プロセス関連文書」その他 手順として、「トレーニング」、「社内wiki」、又は、「その他の実用的な手段」				

※本表はあくまで例。実際に利用しているものとは異なる

インタビューの進め方

- インタビューシートを用意し、Teams会議で画面共有し、ライブで編集しながら進行
- OpenChain仕様要件とその質問項目に沿って聞き取り

次項以降で例を紹介

「SPI専門家とOSS専門家」、「支援対象チームと改善支援チーム」など、
それぞれにおいて、情報の可視化と共有が、相互の理解を深める

インタビューの進め方：組織統括 (マネジメント層) 向けの例

(1.a)(1.b)オープンソースに関するポリシー/
(5.a)-(5c)オープンソースコミュニティ活動への理解・コントリビューション

項番	質問	回答
1.a-1	組織としてOSS活用やOSSコミュニティ参画への方針はありますか？(明文化されていますか？)	
1.a-2	それらは組織メンバに周知されていますか？(組織メンバはそれらの方針を何らかの方法(説明会、教育等)で知らされていますか？)	
1.b	それらの情報は、組織メンバ向けの共有サイト等で公開されていて、組織メンバが必要なときにアクセスできますか？	
5.a 5.c	1には、OSSコミュニティへの貢献に対する方針も含まれていますか？ (方針の程度については、とくに問わない)	
5.b	オープンソースへの貢献を管理する手順書がありますか？	

組織の体制やプロセスの聞き取りは、SPI専門家のスキルに負うところが大だった

※本表はあくまで例。実際に利用しているものとは異なる

インタビューの進め方：開発プロジェクト向けの例

開発プロジェクトの概要把握

	ご担当の開発プロジェクト(プロダクト)について
プロジェクト等名称	• (名称等)
概要	• (目的、技術的特徴、提供経路等々)
所属組織の役割	• (概略：XXXの開発等) (主な取組事項：OSS導入選定、バグフィックス、機能拡張等)
開発関係部署	• (部署名) (関係の概要)
提供先及び提供形態 (可能であれば提供先での 利用態様についても)	• (取引先名)(取引の概要)
そのプロジェクトで 主に利用するOSSなど	• (ディストリビューション、名称、バージョン、ライセンス等)

実態態様とライセンスの把握が、
5230適合におけるライセンスポリシー及びプロセスの評価と策定で重要

※本表はあくまで例。実際に利用しているものとは異なる

インタビューの進め方：開発プジェクト向けの例 (cont'd)

3.a SBOM関連：オープンソースコンポーネントの管理運用の実施手順書 について

項番	質問	ご回答
1	OSSの管理運用の実施手順はありますか	YES or NO （※ Noの場合、(3.a)の以下の項目及び(3.b)はskip)
1-1	OSSを**特定**していますか	YES or NO （※ Noの場合、1-4 へ)
1-1-1	OSSの特定に用いる情報について伺います (例：名称、version、入手元又は提供元、著作権者、ライセンス, etc.)	
1-1-2	特定する情報の収集手段について伺います (※ 自組織について。第三者による支援サービスを利用する場合はそれについても)	誰が： いつ： どのような手段で： その他：
1-2	特定した情報を**確認(承認)**していますか	YES or NO （※ Noの場合、1-4 へ)
1-2-1	確認(承認)の手順について伺います (※ 自組織について。自組織を超えて確認(承認)する場合はそれについて)	誰が： いつ： どのような手段で： どのような観点で： その他：
1-3	確認(承認)した記録を**保管**していますか	YES or NO （※ Noの場合、1-4 へ)
1-3-1	保管の手順について伺います	誰が： いつ： どのような手段で： その他：

※本表はあくまで例。実際に利用しているものとは異なる

ライセンスコンプライアンスは実施できているが、5230仕様とのギャップが存在した

主なギャップ要因の例：

ポリシー、体制、力量、ルール、プロセスについて、暗黙知のものがみられた

一方で、既存のルールやプロセスを大きく見直すまでのものはなく、

明確化でほぼ対応できそうな感触が得られた

明確化とあわせて、可能なものは見直しへ

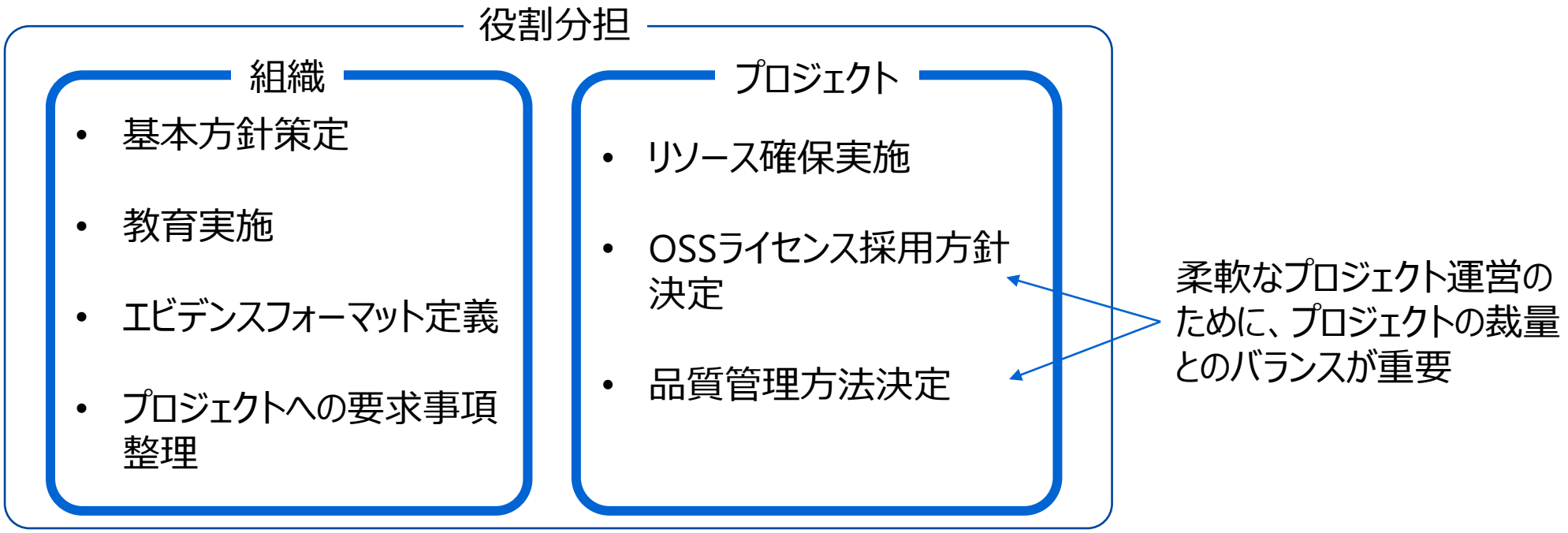
組織とプロジェクトで2階層の体制を構築

改善項目
1. 体制の構築
2. 力量の定義
3. 文書化
4. 教育の実施

- 役割(力量)の定義

  経営者、プログラム責任者、プロダクトリード、照会担当者、ソフトウェア開発者、法務知財窓口、調達窓口、品質管理、オープンソース管理委員会メンバー

- 組織とプロジェクトで役割分担を行い、明確化



改善

明確化に集中できるようにする

改善項目

1. 体制の構築
2. 力量の定義
3. 文書化
4. 教育の実施

- **文書作成及び作業環境**
  - 改善支援チームが**テンプレートを用意**。
    共同編集して作りこむ。
  - 編集作業はGitLab を活用。開発環境に沿う作業環境を選択。
    バージョン管理、変更実施者の把握、進捗管理が円滑
- **SBOM**
  - 管理項目を見直し
    (ex. SBOM管理の動向に留意。取得元情報等を必須項目に)
- **エビデンス管理**
  - 組織として一元管理の徹底

教育：経営層をはじめとする組織全体が積極的に参加

改善項目

1. 体制の構築
2. 力量の定義
3. 文書化
4. 教育の実施

- **説明会**
  - **経営層を含むすべてのメンバーが参加**
  - OpenChain仕様、診断や改善の進捗、策定するポリシーやプロセスが主な話題。関連してのQ&Aを実施。
  - いずれの説明会も、改善支援チームも参加
- **文書の可視化**
  - 開発部門の情報共有サイトでいつでも参照可能

E-Learning による全員参加の教育を実現

改善項目

1. 体制の構築
2. 力量の定義
3. 文書化
4. 教育の実施

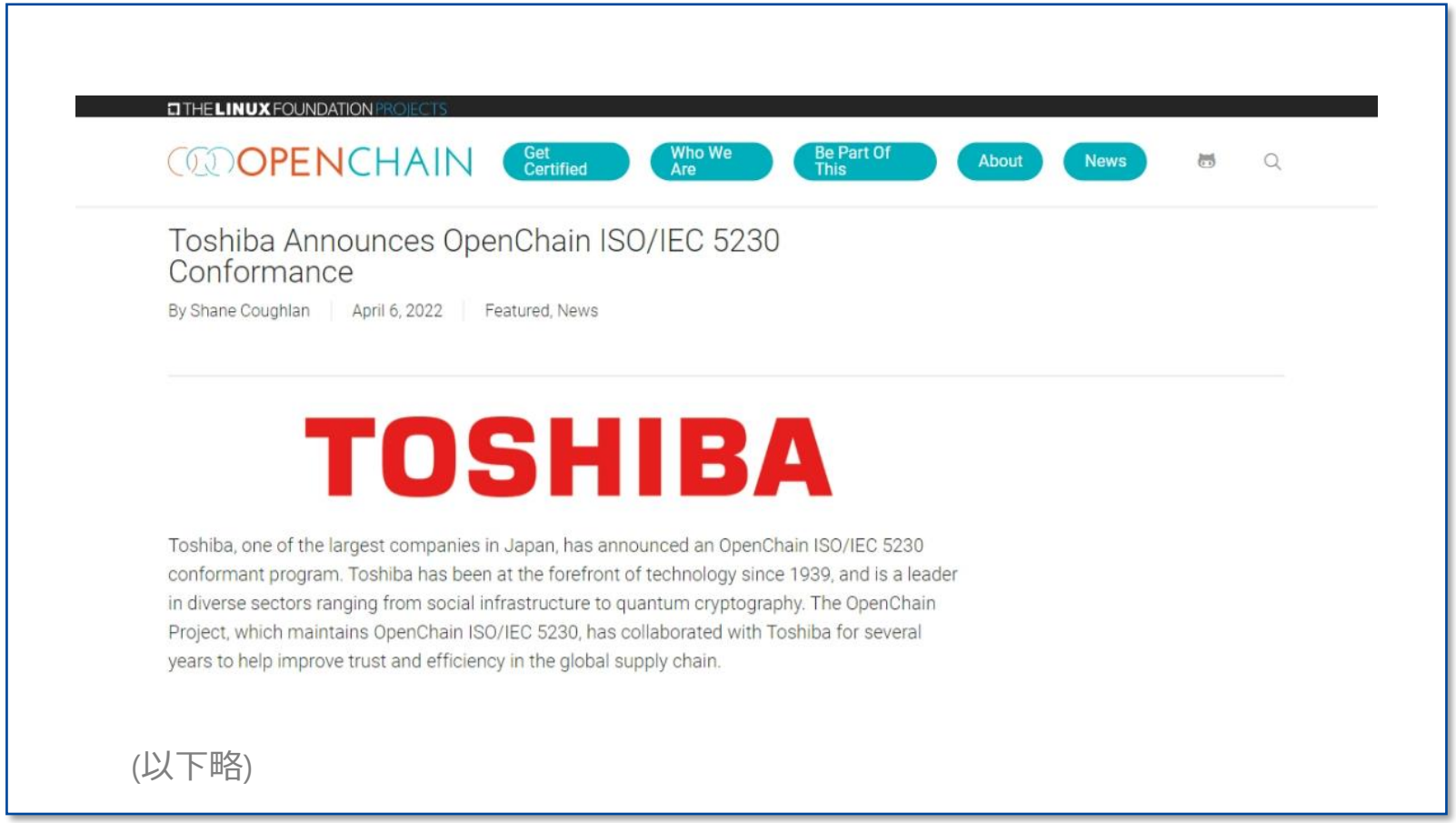
- **E-learning**
  - 2段階にレベル分けした教育コンテンツを改善支援部門が提供*
  - 学習履歴を把握できる

レベル	目的	対象者
入門編	オープンソースソフトウェア(OSS)、オープンソースライセンス、OSSを活用での注意事項などを理解する	プロダクト開発に関係する者は誰でも
基礎編	OSS管理プロセスの重要事項、ワークフロー、注意事項などを理解する	開発、品質保証、知財・法務に従事する者

※ 小山. OSSライセンスコンプライアンスを遵守するためのOSS教育の整備と全社展開.SPI Japan 2022 を参照のこと

（再）評価

質問項目に対してすべてYESと回答できる状態を達成 (2022年2月)



https://www.openchainproject.org/featured/2022/04/06/toshiba-conformance

04

結論

- まとめ
- オープンソース活用とSPI活動
- オープンソース活用と5230適合

まとめ

5230 仕様要件
1. プログラムの基盤（方針や力量）
2. 関連業務の定義と支援
3. オープンソースコンテンツのレビューと承認
4. コンプライアンス関連資料の作成と頒布
5. オープンソースコミュニティ活動への理解
6. （OpenChainの）仕様要件の遵守

SPI専門家

管理方法、組織的な取り組み (力量、教育、ルールの策定等) などの知見を有する。

未知のモデルでも、**既存スキルを軸**にして、**個別モデルの専門家**との**協業**で**対処可**能

OSS専門家

OSSやライセンスなどに関する知見を有する。

とくに要件3と4に関して、インタビューでの聞き取りと課題整理、各種ポリシー策定などの具体的な内容に踏み込んだ検討ができる

- **SPIの診断改善スキルは、5230適合にも有効**
- **OSS活用実態の把握や適合のための検討は、OSS専門家との協業が有効**

オープンソース活用とSPI活動 (オープンソース推進の立場から)

オープンソース活用で、組織力の重要性が高まっている

- コンプライアンスではライセンスなど知的財産や、輸出管理などが論点になりやすい
- OSSを含むソフトウェアサプライチェーンでは、セキュリティ への関心が高まっている
- 経営層の関与、関連部門の連携と支援が重要

SPI は「組織事」として、OSSを含むソフトウェア開発プロセスの改善に取り組める

- 経営層をはじめとする開発現場までの組織の巻き込み力
- CMMI、各種ISO をモデルとするプロセス改善ノウハウ
- 改善という目的に向かう、組織を超えた連携

SPI は、信頼あるソフトウェアサプライチェーンの構築に繋がると確信しています

オープンソース活用と5230適合 (適合組織の立場から)

B2B XaaS 普及の観点から ISO/IEC 5230 は重要

- 5230に準拠したコンプライアンスアーティファクトの流通はOSS管理の基礎に
- 5230適合はソフトウェアサプライチェーンにおける相互信頼の基礎に

OSS管理をより明確な取り組みにできる

- 定期的な見直しによる改善を仕組化できる

「OSSへの貢献」を部門ルールとして明確化できる

- 経営層を含むメンバーの意識や行動にも変化

5230適合は、オープンソースエコシステムへの更なる一歩を後押ししてくれます


TOSHIBA