

OpenChain Projectにおける OSSのTransparency向上への取組

2019/12/4

トヨタ自動車株式会社
知的財産部 IP戦略G
遠藤 雅人

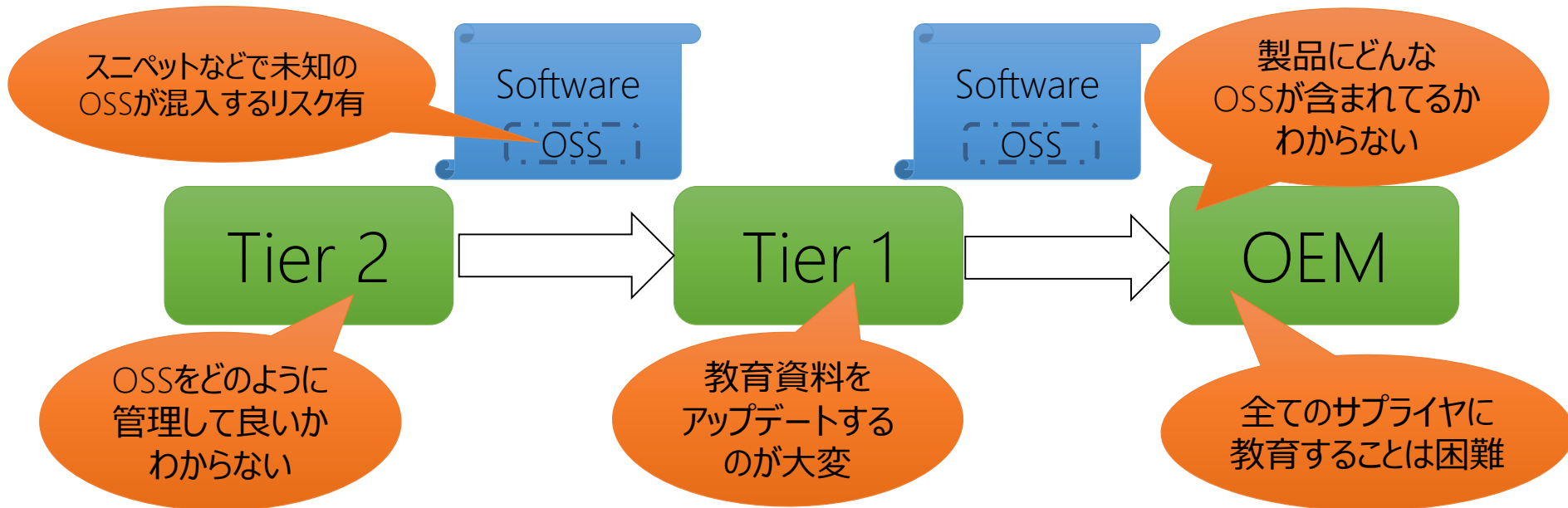
組み込み機器業界のOSS管理の課題

お客様に対してライセンス義務を履行しなくてはならないが、ECUやバイナリで納品される場合にはソフトウェアの中身がわからずどんな義務があるのか把握できない場合有



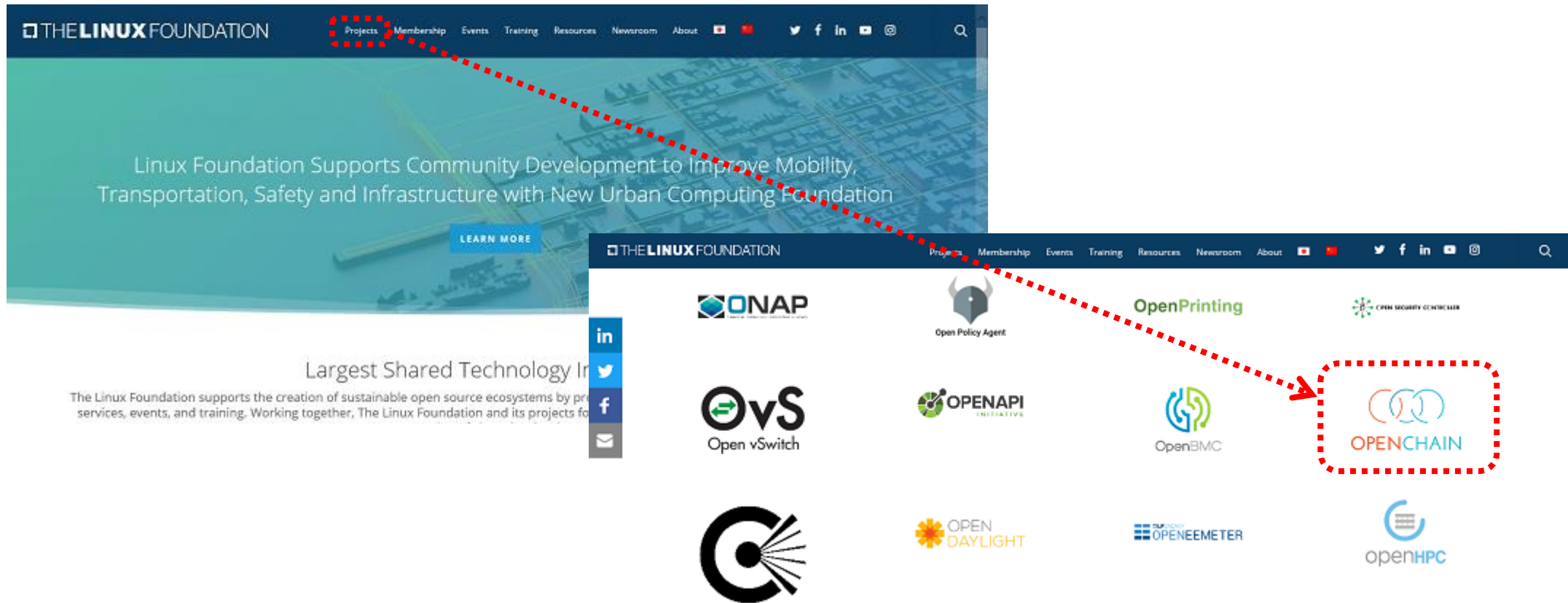
サプライチェーンのライセンスリスク

- ・OSSが紛れ込み、未知の著作権リスクに直面する可能性有
- ・各社の管理体制にバラツキがあるとサプライチェーン全体が脆弱に
- ・各社のガバナンスとSC内でのトレーサビリティ確保が大きな課題に



What is OpenChain Project?

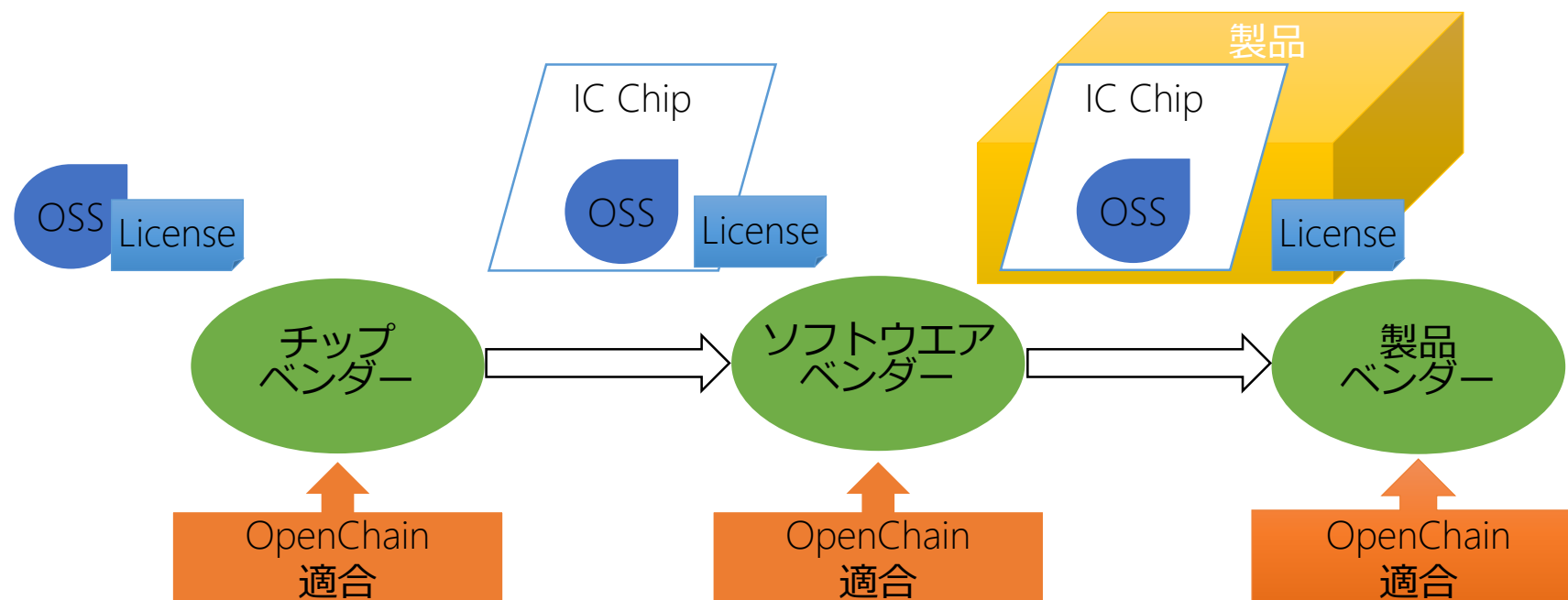
OpenChain ProjectはOSSライセンスコンプライアンスの世界標準の策定・普及を目指すLinux Foundationのプロジェクト



<https://www.linuxfoundation.org/projects/>

OpenChain Projectの目的

OSSサプライチェーン全体にわたる信頼を築くため、各参加者が組織内に確立すべきコンプライアンスプログラムの要件を規定



OSS サプライチェーン(組込機器の例)

OpenChain Projectの3本柱

①仕様(Specification)

企業が組織内に確立すべきコンプライアンスプログラムの要件を定義

<https://wiki.linuxfoundation.org/media/openchain/openchainspec-2.0.pdf>

②適合(Conformant)

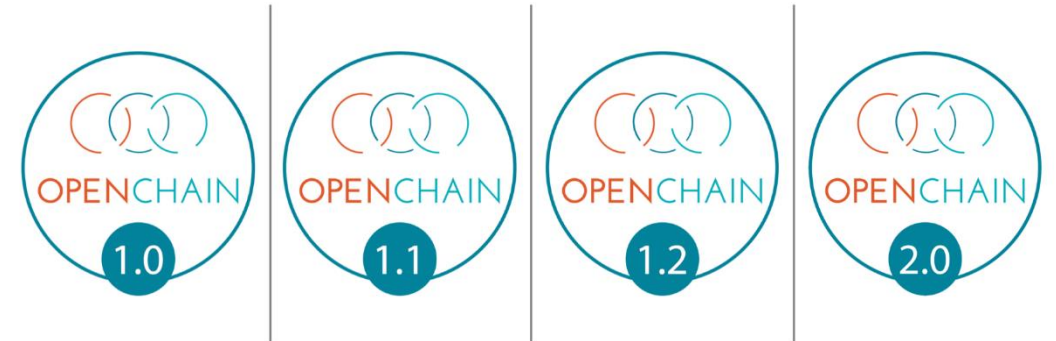
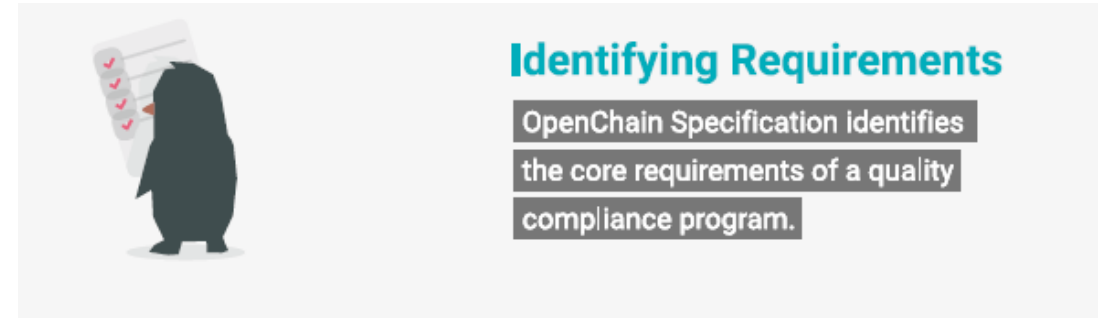
仕様に適合しているか否かをWebアンケートで回答することで、認証を取得可能
原則、自己認証だが第三者認証も有

<https://www.openchainproject.org/get-started/conformance>

③カリキュラム(Curriculum)

仕様への適合のために各社内で利用可能な教育資料集

<https://www.openchainproject.org/resources>



Reference Open Source Training Slides for OpenChain 2.0

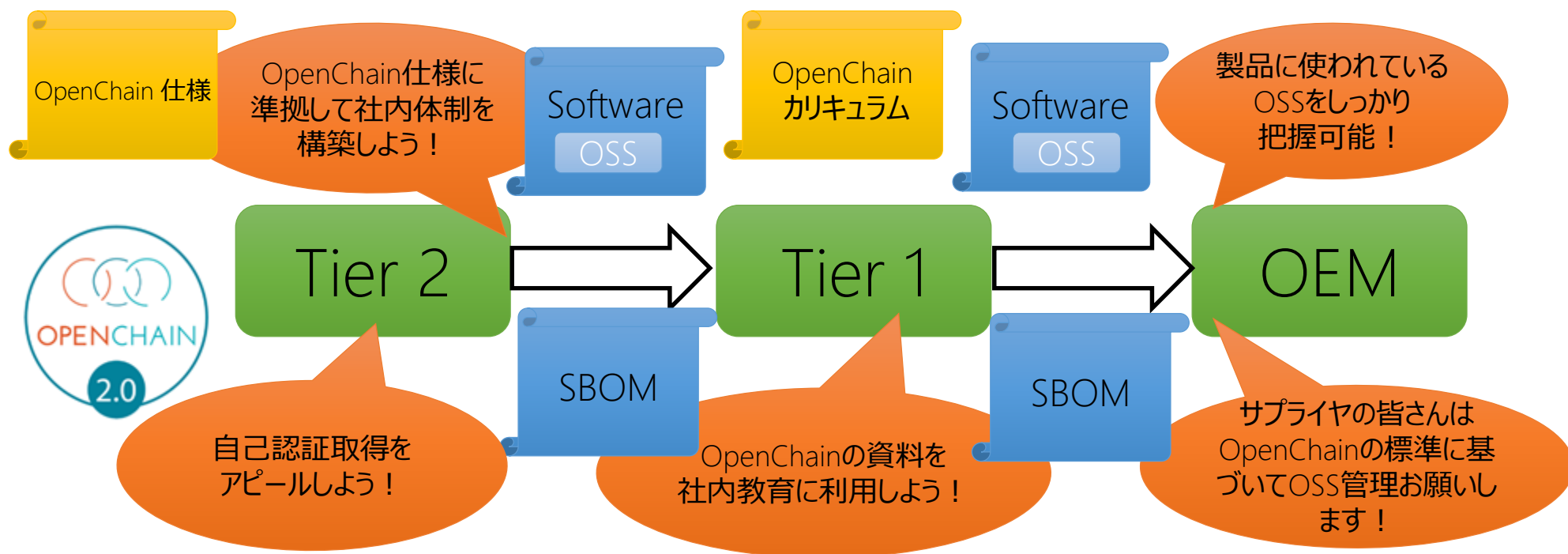
Released under CC0-1.0.
You may use, modify, and share these slides without restriction.
They also come with no warranty.

These slides follow US law. Different legal jurisdictions may have different legal requirements. This should be taken into account when using these slides as part of a compliance training program.

These slides do not contain legal advice

OpenChain採用のメリット

各社がOpenChain Specificationに基づいて社内体制を構築することでサプライチェーン全体が強固なものに



Platinum Members



BOSCH



facebook



Panasonic



SIEMENS

SONY

TOSHIBA

TOYOTA

Uber

Western Digital.

<https://www.openchainproject.org/about/members>

Community



Mark Gisi
Specification Chair
[LinkedIn](#)



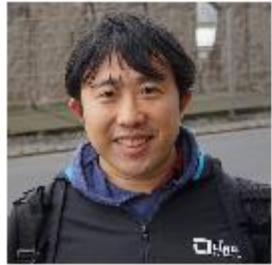
Miriam Ballhausen
Conformance Chair
[LinkedIn](#)



Alexios Zavvas
Curriculum Chair
[LinkedIn](#)



Nathan Kumagai
Onboarding Chair
[LinkedIn](#)



Masato Endo
Automotive Chair
[LinkedIn](#)



Oliver Fendt
Tooling Chair
[LinkedIn](#)



Gary O'Neill
Lead Developer
[LinkedIn](#)



Catharina Maracke
Strategic Advisor
[LinkedIn](#)



Matija Suklje
Strategic Advisor
[LinkedIn](#)



Indira Bhatt
Community Representative
[LinkedIn](#)



Dave Marr
Governing Board Chair
[LinkedIn](#)



Shane Coughlan
General Manager
[LinkedIn](#) / [Facebook](#) / [Twitter](#)



Kelly Williams
Secretary Emeritus

<https://www.openchainproject.org/about/leaders>

OpenChain SpecにおけるSBOMの取扱

SBOMを作成・管理する社内プロセスを持つことを義務付けている

Spec 2.0 仮訳

3.1部品表 (Bill of Materials)

供給ソフトウェアを構成するオープンソースコンポーネント（および、確認ライセンス）を含む部品表を作成し、管理するプロセスが存在すること。

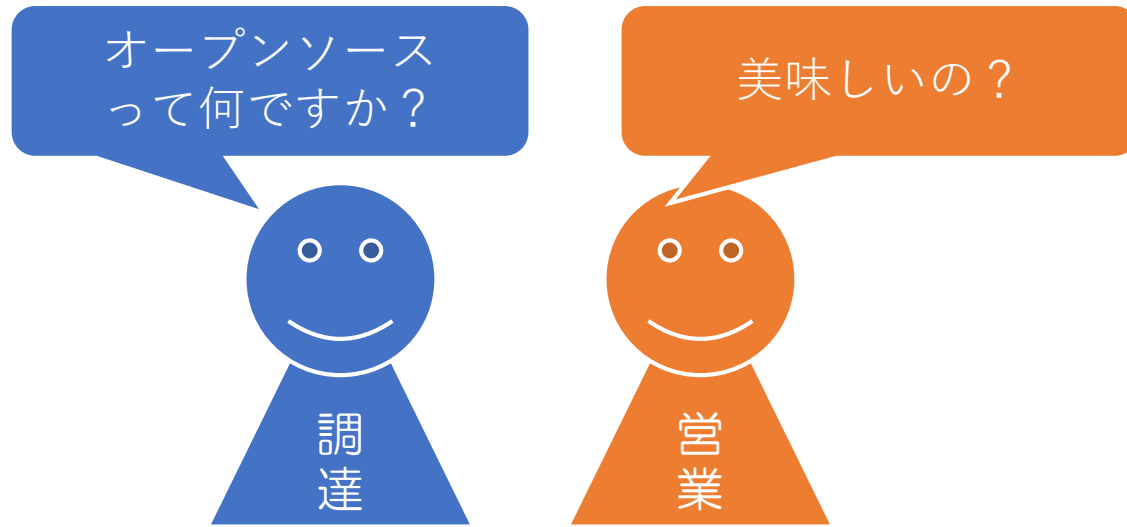
証跡となる資料

3.1.1 供給ソフトウェアを構成するオープンソースコンポーネントの集合を、特定し、追跡し、レビューし、承認し、情報保管する、文書化した手順。

3.1.2 供給ソフトウェアに対し、文書化した手順が適切に運用されたことを示す、オープンソースコンポーネントの記録。

<https://wiki.linuxfoundation.org/media/openchain/openchainspec-2.0.pdf>

SBOM共有にあたって日本企業が直面した課題



取引契約を行う担当者が
OSSを知らない

⇒ 契約にSBOMに関する
条項が織り込まれない

SBOMのフォーマットがバラバラ

⇒ ・各社での管理が煩雑に
・テクニカルなフォーマット
だと法務/知財が取扱えない

OpenChain Japan WG

ベストプラクティスの共有や、共通課題の解決を図るため
2017年12月にソニー/日立/トヨタの3社が設立

⇒国内70社/170名以上が参加し、国別WGのモデルケースに
7つのSub WGが活動中「日本語で議論し、英語でアウトプット」

SUB Working Groups

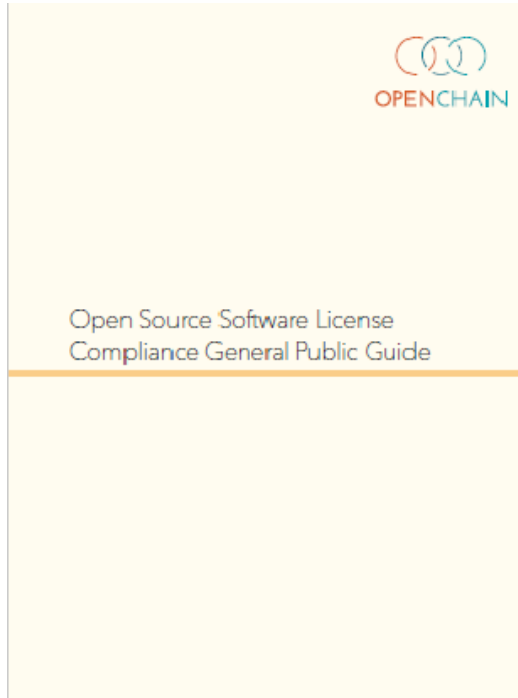
- Planning SWG
- FAQ SWG
- Leaflet to Supplier SWG *
- Education material for roles SWG
- License information exchange SWG *
- Tooling SWG
- Promotion SWG

* Transparency向上に関わるSWG



Leaflet to Supplier SWG

営業/調達/法務/経営者など普段OSSにあまり関わらない人々に
OSSライセンスコンプライアンスの重要性を周知するリーフレットを作成



国内外のイベント配布

- Automotive Linux Summit
- Open Source Conference
- 関西オープンフォーラム
- Open Source Summit North America
- Embedded Linux Conference
- Debconf @ Brazil
- Open Culture Foundation Taiwan Workshop

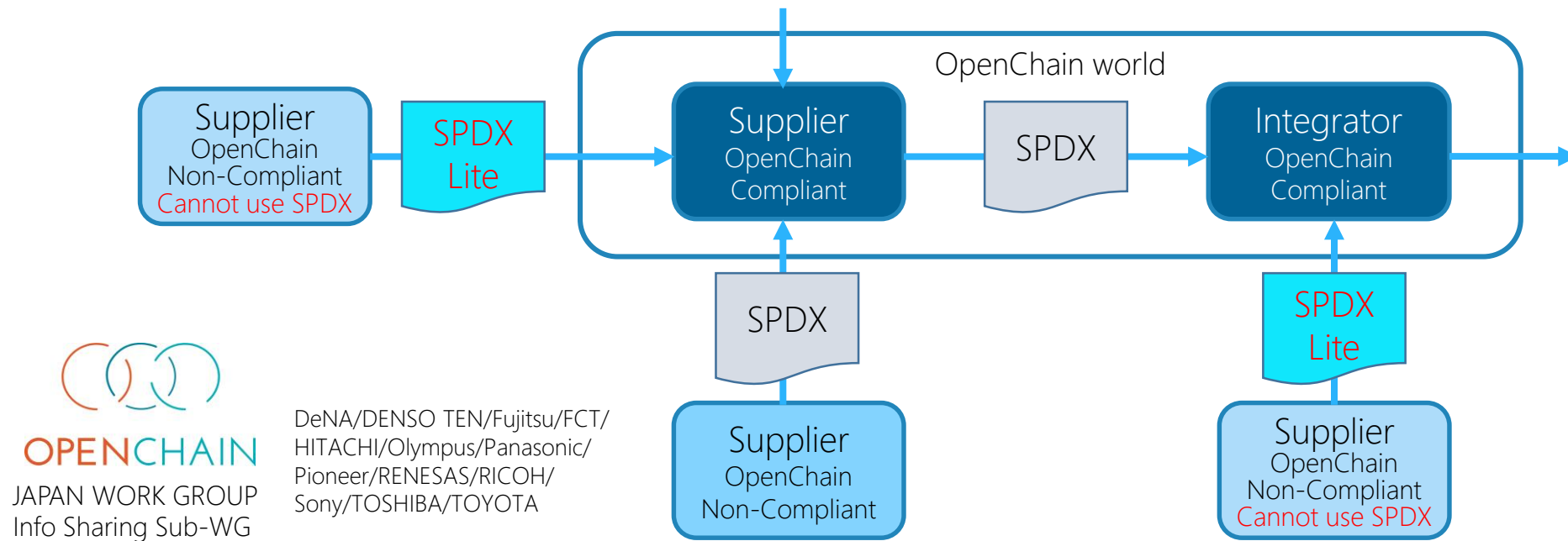
(日本語版) <https://github.com/OpenChain-Project/curriculum/blob/master/supplier-leaflet/supplier-leaflet-1.0-jp.pdf>

(英語版) <https://github.com/OpenChain-Project/curriculum/blob/master/supplier-leaflet/supplier-leaflet-1.0-en.pdf>

* 簡体字版、繁体字版も完成済、上記サイトにアップロード予定

License information exchange SWG

SPDXのハンドリングが困難な組織でもSBOMを取扱可能にする
入門編のSPDX Liteを定義。Excelで気軽に扱え、ツールとの互換性も確保。
日本からSPDXコミュニティに提案し、SPDXの1フォーマットとして
採択される見込。



https://wiki.linuxfoundation.org/openchain/jwg_license_sg_page

SPDX Lite

ライセンスコンプライアンスを行う上で最低限必要な項目に絞ったSBOM。情報の完全性よりも運用性の高さを重視し、足りない情報があれば、再問合せして補完することを想定。

SPDX Liteの項目例	-パッケージダウンロード位置（入手先）	-ライセンスへのコメント
-パッケージ名	-解析したファイル（手作業の場合false）	-著作権テキスト
-パッケージSPDX識別子	-ホームページ（開発コミュニティサイト）	-改変の有無
-パッケージバージョン	-結論されたライセンス	-パッケージに関するコメント
-パッケージファイル名	-宣言されたライセンス	-ライセンス識別子

SPDXサンプルの一部抜粋									
	3.1	3.2	3.3	3.4	3.7	3.8	3.11	3.13	3.15
	PackageName	Package SPDX Identifier	Package Version	PackageFileName	PackageDownloadLocation	Files Analyzed	PackageHomePage	Concluded License	Declared License
項	パッケージ名	パッケージSPDX識別子	パッケージバージョン	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ト）	結論されたライセンス	宣言されたライセンス
	LibXML2		2.99	libxml2-2.9.9.tar.gz	ftp://xmlsoft.org/libxml2/	FALSE	http://xmlsoft.org/	MIT	MIT
	PCRE		8.4343	pcre-8.43.tar.gz	ftp://ftp.pcre.org/pub/pcre/	FALSE	https://www.pcre.org/	BSD-3-Clause	BSD-3-Clause
	SQLite		3300100.t artar	sqlite-autoconf- 3300100.tar.gz	https://www.sqlite.org/download.html	FALSE	https://www.sqlite.org/index.html	その他（ライセンス名を記載）	その他（ライセンス名を記載）
	Zlib (1.2.3)		1.2.11	zlib-1.2.11.tar.gz	https://www.zlib.net/	FALSE	https://www.zlib.net/	Zlib	Zlib
	cURL (7.41.0)		7.66.0	curl-7.66.0.tar.bz2	https://github.com/curl/curl/releases	FALSE	https://curl.haxx.se/	MIT	MIT

<https://github.com/OpenChain-Project/Japan-WG-General/tree/master/License-Info-Exchange>

OpenChain Automotive WG

- ・ 2019年7月にトヨタの呼びかけで設立したグローバルな業種別WG
- ・ 日米欧韓の12の自動車会社を含む100名以上がメンバー登録
- ・ 日本、欧州で会合を実施し方向性を議論、次回は米国（20年1月）

初回会合 2019/7 Automotive Linux Summit @ Tokyo

WGの三つの目的を確認

- ①自動車業界内のベストプラクティスを共有
- ②OSS SCMの自動車業界標準の検討
- ③OSSコンプライアンスの重要性の業界内での周知活動



<https://www.openchainproject.org/news/2019/07/15/openchain-automotive-work-group-a-global-solution-for-a-global-market>

第2回会合 2019/10 Open Source Summit Europe @ Lyon

Scania/Bosch/富士通/デンソーテンの4社から
各社における取組の紹介を実施

⇒OpenChain適合やSPDX/SPDX Lite等についても議論



<https://www.openchainproject.org/featured/2019/11/13/openchain-automotive-work-group-meeting-2-outcomes>

今後の取組① CES2020

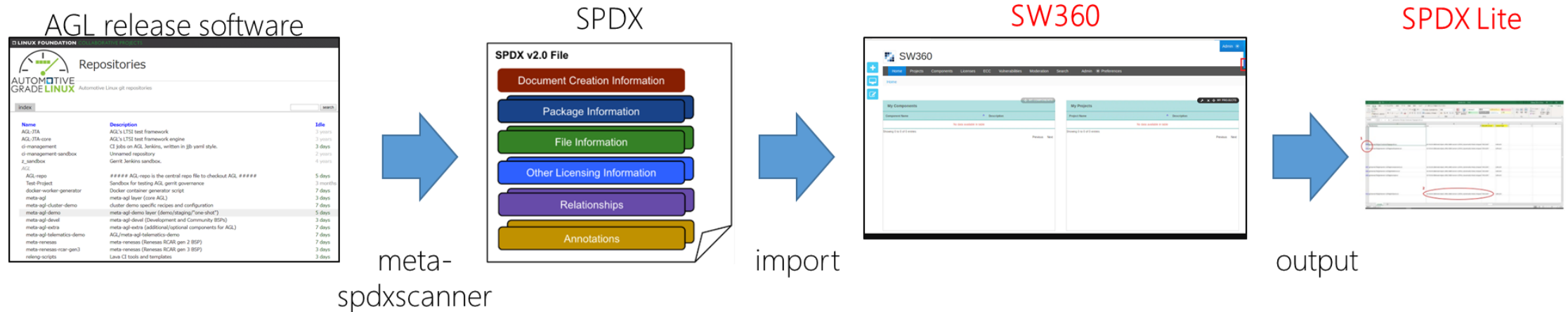
Auto WGの3回目の会合に加え、AGLブース内にOpenChainコーナーを設置

第3回会合 2020/1 Consumer Electronics Show @ Las Vegas

GM/トヨタ/ソニー等からプレゼンを行い、2020年の活動計画を検討予定

Automotive Grade Linux (AGL) × OpenChain @ CES2020

AGLのリリースソフトのSBOM化 (SPDX/SPDX Lite) のデモやリーフレット配布を実施予定



今後の取組② OpenChainのISO化

- ・ OpenChainプロジェクトは仕様(Ver2.1)のISO化を推進
Joint Technical Committee 1 (JTC-1)に
Publicly Available Specification (PAS) として提出
- ・ 現在、仕様(Ver2.1)についてのパブコメを募集中（12月10日まで）

https://wiki.linuxfoundation.org/openchain/openchain-specification-wiki-page?&#specification_developmentrelease_process

- ・ 標準化経験が豊富なJoint Development Foundationと共に
作業を進め2020年を目標にISO化を目指す

今後の取組③ SPDX3.0（次期仕様）

よりSBOMとしての実用性を高めるために新項目の追加を検討中

SPDX3.0 追加検討項目

- Security
- Pedigree
- Provenance
- Export

OpenChain/SPDX等のOSSコンプライアンスに関する検討は
12月に東京で行われる下記イベントでも行われる予定



<https://events19.linuxfoundation.org/events/open-compliance-summit-2019/>



Japan Work Group 第12回全体会合 @ NEC (田町)

12月19日（木）13:30-18:00

一般の方の参加方法は下記サイトの12/3の投稿ご参照

<https://qiita.com/advent-calendar/2019/openchainjapanSWG>

Thanks