Open Source Governance and Supply Chain Management with Community

Masato ENDO

Introduction

- Set up Open Source Governance Structure of TOYOTA @IPD
- Automotive Chair of OpenChain Project
- Leader of Promotion SG of OpenChain Japan WG
- A manager of software & value chain service development of TOYOTA

Contact masato_endo@mail.toyota.co.jp
http://linkedin.com/in/masato-endo-279026159

Why does TOYOTA want to acquire OpenChain certification? (1)

▼Full model change to a MOBILITY COMPANY

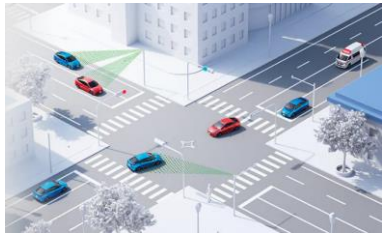
⇒The concept **"SOFTWARE FIRST"** which separates hardware from software and develops software in advance is expanding.

Release a connected city project at CES2020 (January, 2020)

Collaboration with NTT (March, 2020)

OSS usage is expanding rapidly

MOBILITY TEAMMATE CONCEPT
Automated Driving Tech.



Example

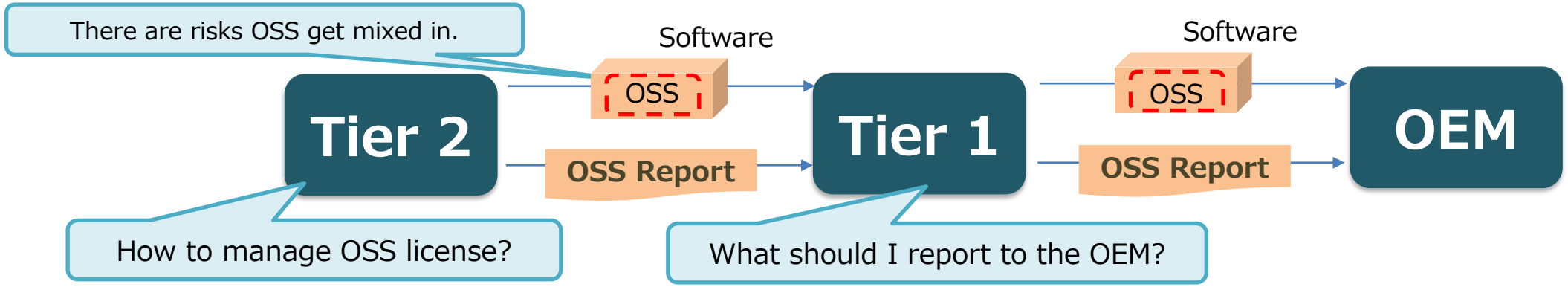
AUTOMOTIVE GRADE LINUX

We're promoting Automotive Grade Linux（AGL）which develops Linux for Automobiles as a platinum member.
⇒We promote **reducing IP Risks** for promoting AGL.

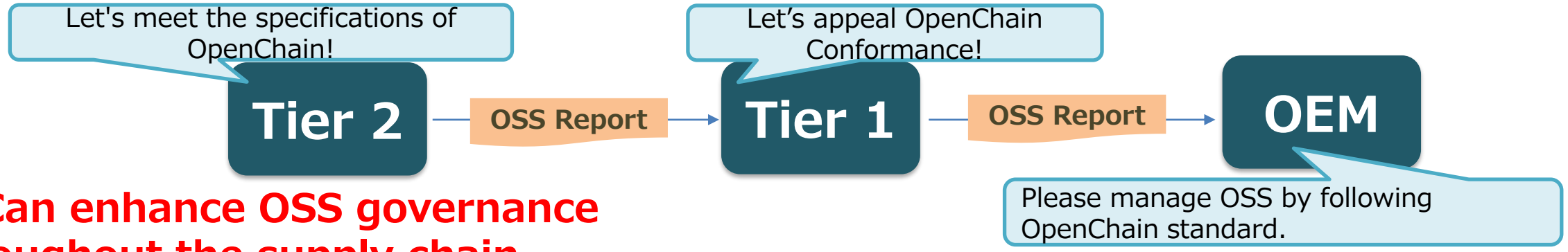
AGL was commercialized at first as an IVI system in the summer of 2017

Why does TOYOTA seek OpenChain certification? (2)

▼ Problems specific to the automobile industry



▼ Each company establishes a management system based on the OpenChain standard



⇒ Can enhance OSS governance throughout the supply chain

OpenChain Japan WG

Hitachi, Sony and Toyota set up Japan WG in 2017.
Each Sub-WG makes materials for OSS compliance and uploads to GitHub.

SWG participants
Event speakers
~50 people

Bimonthly meeting
~100 people

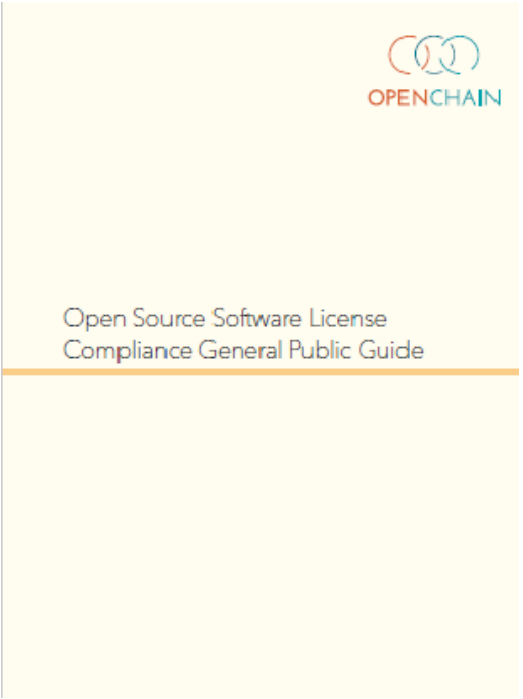
ML subscribers
200+ people

SUB Working Groups
- -Planning SWG
- -FAQ SWG
- -Leaflet to Supplier SWG
- -Education material for roles SWG
- -License information exchange SWG
- -Tooling SWG
- -OSPO SWG
- -Promotion SWG

https://github.com/OpenChain-Project/Onboarding-JWG

Example of output of WG (1)

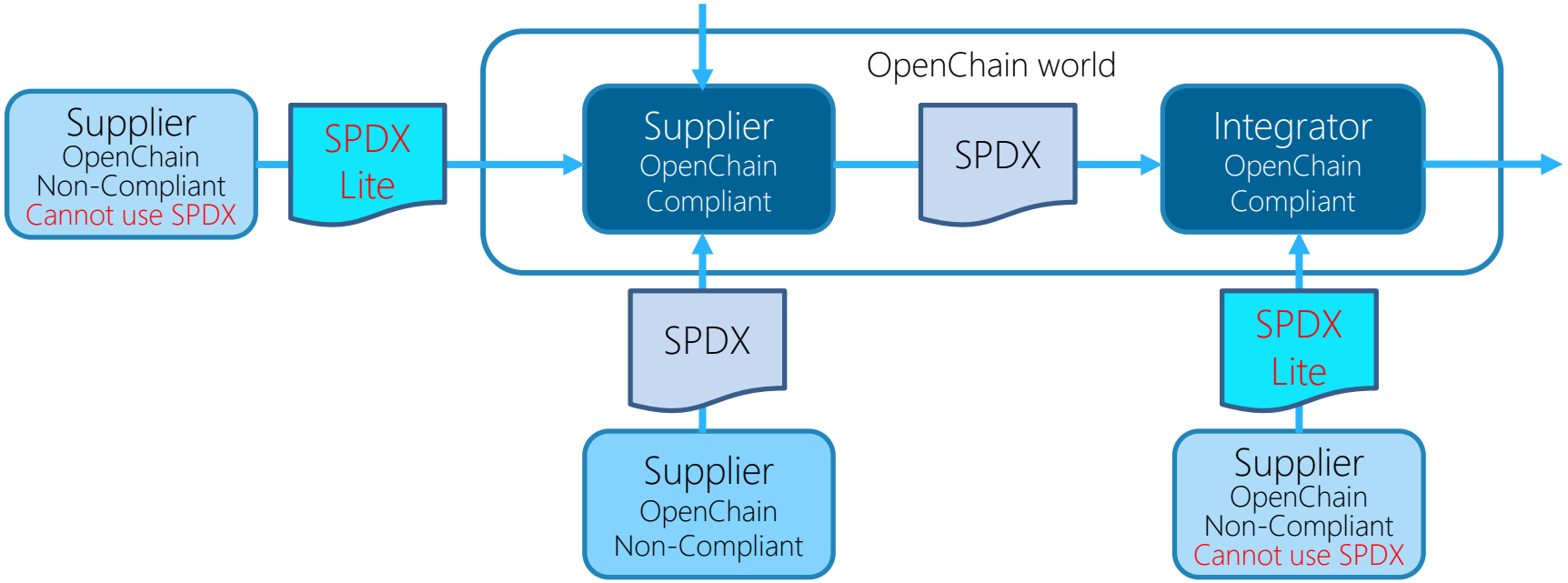
Leaflet to Supplier SWG made
“Open Source Software License Compliance General Public Guide”
tell as many people as possible about the basic principles of OSS.



https://github.com/OpenChain-Project/Reference-Material/tree/master/Suppliers/Leaflet/Official/2.0

Example of output of WG (2)

License information exchange SWG defined SPDX Lite (ex. OSS Package Info). It would be an efficient way to manage supply chains where some suppliers cannot use the full SPDX specification. SPDX lite became one of profiles of SPDX2.2 which is ISO version of SPDX.



Example of output of WG (3)

Interview with Masato Endo, OpenChain Project Japan

Linux Foundation Editorial Director Jason Perlow had a chance to speak with Masato Endo, OpenChain Project Automotive Chair and Leader of the OpenChain Project Japan Work Group Promotion Sub Group, about the Japan Ministry of Economy, Trade and Industry's (METI) recent study on open source software management.

JP: Greetings, Endo-san! It is my pleasure to speak with you today. Can you tell me a bit about yourself and how you got involved with the Japan Ministry of Economy, Trade, and Industry?

遠藤さん、こんにちは！本日はお話しできることをうれしく思います。あなた自身について、また経済産業省とどのように関わっていますか?

ME: Hi, Jason-san! Thank you for such a precious opportunity. I'm a manager and scrum master in the planning and development department of new services at a Japanese automotive company. We were also working on building the OSS governance structure of the company, including obtaining OpenChain certification.

https://www.linuxfoundation.org/blog/interview-with-masato-endo-openchain-project-japan/

METI Ministry of Economy, Trade and Industry

Contact Us | Japanese | Site Map | Main Content | Font size S M L | Easy Web Browsing

News Releases | Speeches | Statistics | Policies | About METI

Home ▶ News Releases ▶ Back Issues ▶ April FY2021 ▶ Collection of Use Case Examples Compiled Regarding Management Methods for Utilizing Open Source Software and Ensuring Its Security

Japanese | Print

Collection of Use Case Examples Compiled Regarding Management Methods for Utilizing Open Source Software and Ensuring Its Security

April 21, 2021

▶ Manufacturing, Information, and Distribution/Service Policy

The Ministry of Economy, Trade and Industry (METI) publishes a "Collection of Use Case Examples Regarding Management Methods for Utilizing OSS and Ensuring Its Security." The collection summarizes the points to note when utilizing open source software (OSS), and for each point, provides information including use case examples of companies that are conducting instructive initiatives.

1. Background and purpose

On September 5, 2019, METI inaugurated a Task Force for Evaluating Software Management Methods, etc. toward Ensuring Cyber/Physical Security (Software Task Force), placing it under the Cross-sectoral Sub-Working Group of the Study Group for Industrial Cybersecurity's Working Group 1 (WG1). The Software Task Force has been examining appropriate software management methods, responses to vulnerability and license issues, etc. ever since.

The importance of software in industry has grown in recent years, and is now used to control industrial machinery and automobiles. In addition, developing systems on generic hardware will enable software to perform a variety of functions, and this in turn is expected to create various kinds of value added.

In particular, the source code for OSS is accessible to the public and available to be used, modified, and redistributed for both commercial and non-commercial purposes. Therefore, OSS is being actively used in commercial products and services, particularly in General Utility Library Programs, etc. It is now difficult to create products and services without using OSS.

https://www.meti.go.jp/english/press/2021/0421_003.html

Example of output of WG (4)

Promotion SWG plans “OpenChain Japan Advent Calendar” every year.
And, from 2022, we’re collaborating with Japanese tech media.

日	月	火	水	木	金	土
28	29	30	1 @AyumiWatanabe Happy Holidays from OpenChain JapanWG	2 @owada-k 今年のOpenChain Japan Work Groupの活動まとめ / Summary of OpenChain Japan Work Group Activity in 2021	3 @n-shima OpenChain 認証企業 ふえてます / The number of openchain certified companies is increasing.	4 @koizumistr OpenChain Japan Work Groupへの参加方法/How to participate OpenChain Japan Work Group
5 @MasatoENDO 東京都オープンソース公開ガイドラインについて　About Tokyo OSS Guideline	6 @tks 技術評論社のwebに中国でのCompliance-Sigの記事を書きました！	7 @AyumiWatanabe ソフトウェアの透明性とSBOMについて(Software Transparency and SBOM)	8 @zp_takashi SPDX Documentを理解する	9 @zp_takashi SPDX-LiteでSBOMを作ってみよう	10 @nori0428 SPDX® が ISO/IEC 5962:2021 として公開されました / SPDX® became ISO/IEC 5962:2021	11 @nori0428 SPDX Podcast !!
12 @MasatoENDO 経産省のOSS管理手法事例集について　About METI's Case Study of Open Source Management Methods	13 @MasatoENDO 続OSSスキル標準について　Open Source Skill Standard	14 @MasatoENDO OpenChain Security Assurance Reference Guide	15 @kida_oss OpenChain Security Assurance Reference Guideの翻訳について	16 @ogojo OpenChain Japan work group FAQ subgroup 最新状況のご紹介／Latest Status Update	17 @ambai OSSコンプライアンスに関連するプロジェクトやツールの紹介	18 @hiromotai7 meta-spdxscannerを試してみた
19 @AyumiWatanabe Event Report of OSS Management Forum 2021	20 @keiya-nobuta ライセンス コンプライアンスについてのOSSJ 2021 富士通セッションサマリ / OSSJ 2021 Fujitsu session summary about license compliance	21 @ShinsukeKato Open Source Summit Japan イベントレポート	22 @_hfukuchi Open Source Summit Japan 2021 Report: OSPOの役割について／Roles of OSPO	23 @gucci56 Open Compliance Summit 2021 参加レポート	24 @TakashiNinjouji オープンソースコンプライアンスの透明性と相互運用性からオートメーションに向けて / From Transparency and Interoperability to Automation in Open Source Compliance	25 @MasatoENDO OpenChain JWG: 25日間のまとめと2022の展開について

https://qiita.com/advent-calendar/2021/openchainjapanwg

解決！OSSコンプライアンス

「OSSはただの無料ソフト」「うちの会社に関係ない」。まだ、こうした考えを持っている企業は多い。だが、ソフトウェアをビジネスの武器にしようとしている企業は、OSSの利用を避けることはできない。利用を適切に管理しないと、思わぬ法的トラブルに巻き込まれる可能性がある。 この連載ではOSSコンプライアンスに関する具体的な課題と解決策をひも解いていく。

https://atmarkit.itmedia.co.jp/ait/series/27403/

OSSのサプライチェーン管理、取るべきアクションとは

OSSのサプライチェーン管理の重要性に関する認識が高まっている。本連載では、この文脈から「オープンソースプログラムオフィス（OSPO）」「SBOM」の2つのキーワードを取り上げ、解説と座談会でその世界に迫る。

https://atmarkit.itmedia.co.jp/ait/series/30163/

Issues for acquiring OpenChain certification (1)

Issue (1)

I understand the conditions required to obtain certification, but I don't know what to start with.

▼Define the documents required for certification

TOYOTA OpenChain Packages(TOCP)

①	Toyota Open Source General Policy	⑧	OSS Approval List
②	Toyota Open Source Contribution Policy	⑨	OSS Organization Chart
③	Practical Rules for OSS Compliance	⑩	Contribution Check List
④	OSS Compliance Guide Line	⑪	Toyota Open Source Program
⑤	OSS Process	⑫	OpenChain Specification Declaration of certification
⑥	OSS evidence format	⑬	List of roles and capabilities
⑦	OSS Manual	⑭	OSS Program Ability Evidence Document

*Centralize information on the in-house website
Always shared within the organization

Issues for acquiring OpenChain certification (2)

Issues(2) 3.2 Management program

Because there are engineers in various positions in the company, one business process / manual cannot cover all

What should I do when supplier uses OSS?

I want to use OSS for in-house tools

I want to use in house development to embed OSS in a car

I'd like to contribute to OSS Community.

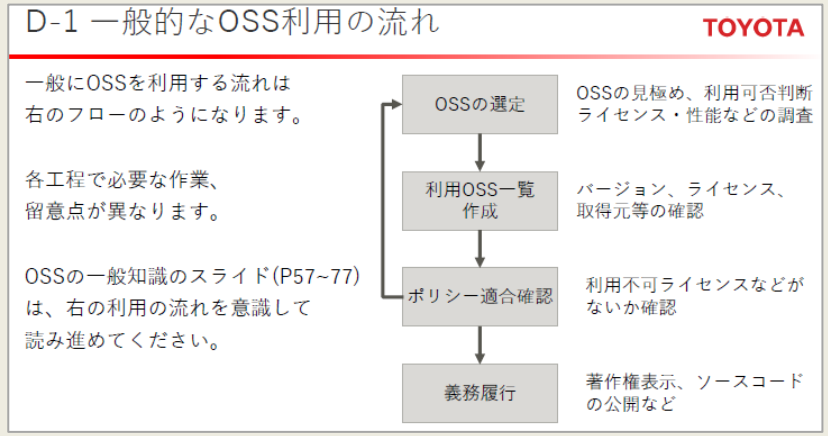
▼Establish a process for each development form / contribution

①In-house development

②Supplier development

③R&D, Tools

④Contribution



Issues for acquiring OpenChain certification (3)

Issues(3) 3.1 BoM Process

I don't know how to manage OSS information

What format should I use to manage it?

▼Established OSS evidence format for each development form

In-house development

Supplier development

R&D Tools

↑List the person in charge, approver, and author on the front page as evidence that the process was successful.

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	ライセンスへのコメント	著作権テキスト
ex1	linux-renesas	SPDXRef-upload392	4.14.75	linux-renesas-4.14.75+gitAUTOINC+a5268d2981-r1-	git://gitkernel.org/pub/scm/linux/kernel/git/horms/renesas-bsp.git	meta-spdxscanner		GPL-2.0-only			
ex2	gstreamer1.0	SPDXRef-upload245	1.12.2	gstreamer1.0-1.12.2-r0-patched.tar.gz	http://gstreamer.freedesktop.org/src/gstreamer/gstreamer-1.12.2.tar.xz	meta-spdxscanner	http://gstreamer.freedesktop.org/	LGPL-2.0-only			
ex3	kernel-module-mmngr	SPDXRef-upload247	1	kernel-module-mmngr-1.0-r0-patched.tar.gz	git://github.com/renesas-rcar/mmngr_drv.git	meta-spdxscanner		MIT	GPL-2.0-only		
1											
2											
3											
4											
5											
6											
7											

↑ We use SPDX Lite format defined by OpenChain Japan WG

Issues for acquiring OpenChain certification (4)

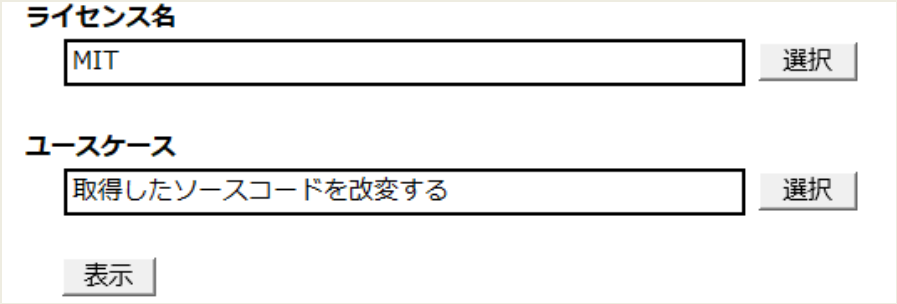
Issues(4) 1.3 Review Process

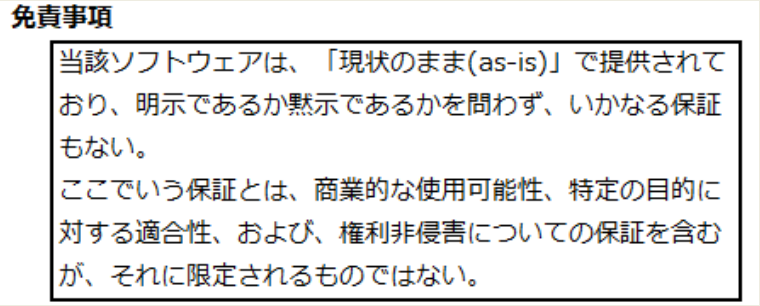
It takes time to understand the license

Can I use this license? ??

It takes time to read the license texts one by one.

▼Using Simple OSS License Viewer



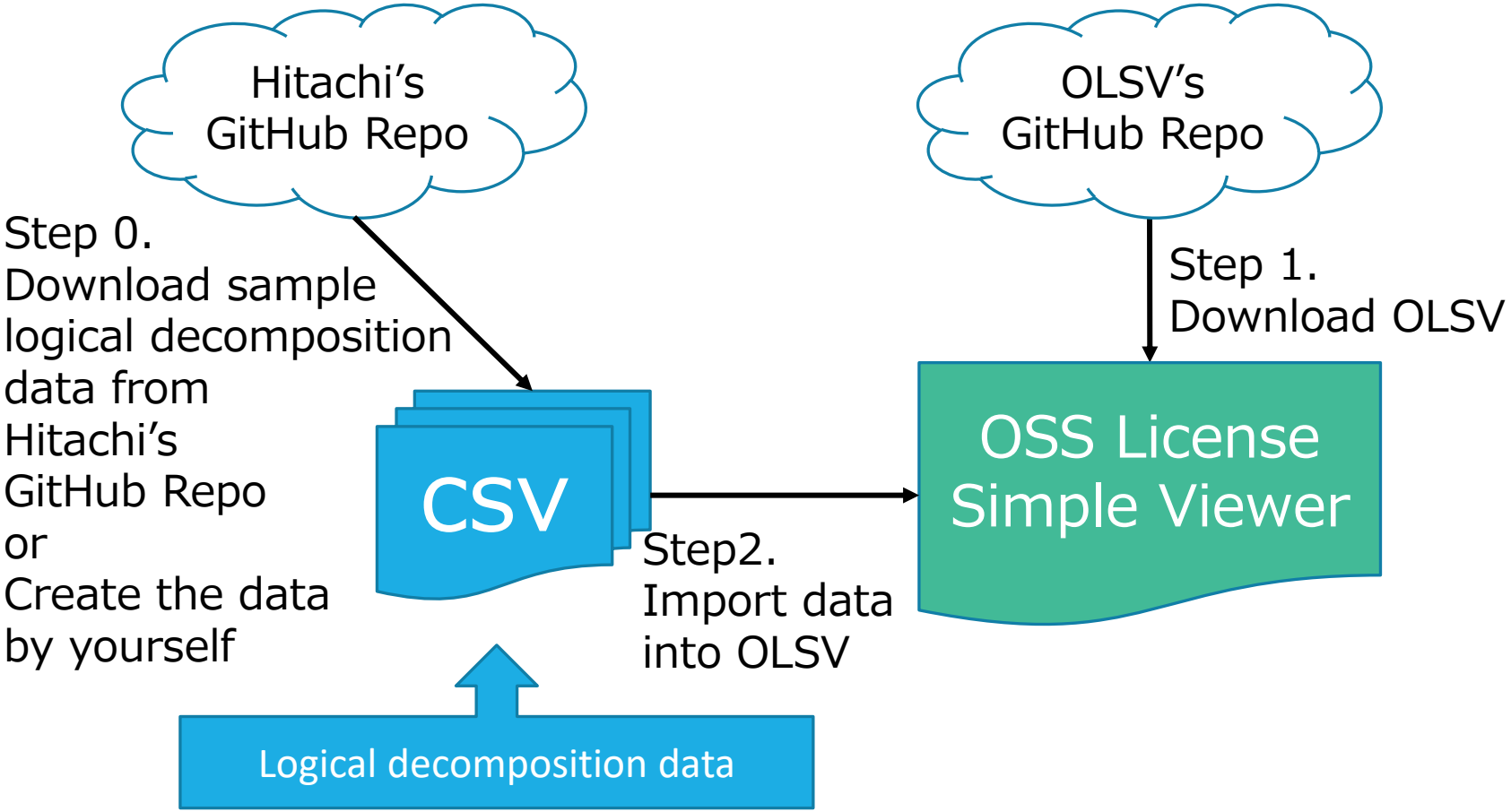


⇒You can easily grasp the responsibilities and disclaimers described without reading all the license texts.

*Use the "in-house license database" to check conformity with the in-house policy

You can get OSS License Viewer at our Github repo: https://github.com/OLSV-oss/OSSLicenseSimpleViewer

Structure of OSS License Simple Viewer



I am using GPL v2 license in my commercial products. According to OLSV, I need to distribute the corresponding source code. It's clear now!

Issues for acquiring OpenChain certification (5)

Issues(5) 1.2 Education

We want people who are not familiar with software development such as procurement and sales to understand the necessity of business.

Procurement and Sales

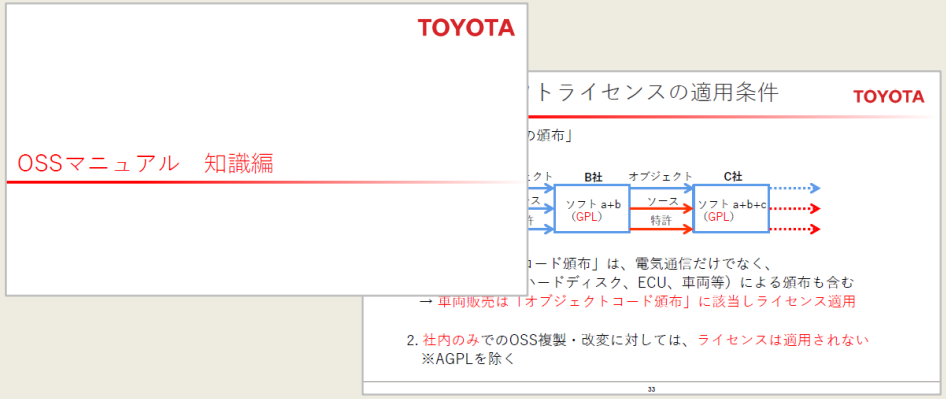
What is OSS?
Why do I have to deal with it?

▼Prepare educational content that suits each level

①For ALL

Easy-to-understand explanation of basic knowledge about OSS by e-learning
⇒ Over 16,000 people took the course

②For engineers



Hold an online course for practitioners with detailed license knowledge
⇒Confirmation test will be conducted after the course

Toyota became the first company to announce adoption of ISO / IEC 5230.

Toyota Is The First Company To Announce Adoption Of ISO/IEC 5230, The International Standard For Open Source Compliance

By Shane Coughlan | December 15, 2020 | Featured, News

TOYOTA

Toyota announces adoption of ISO/IEC 5230 in the IP Planning Group, a process led by Masato Endo and Miyu Tanaka. ISO/IEC 5230 is the International Standard for open source compliance.

ISO/IEC 5230 is maintained by the OpenChain Project as OpenChain 2.1 and edited for ISO via the Joint Development Foundation OpenChain Working Group. ISO/IEC 5230 is supported by Arm, BMW CarIT, Bosch, Cisco, Comcast, Facebook, Fujitsu, Google, Hitachi, Microsoft, MOXA, OPPO, Panasonic, Qualcomm, Siemens, Sony, Toshiba, Toyota, Uber and Western Digital as governing board members, and a wide community of companies across three continents.

OPENCHAIN 2.1

https://www.openchainproject.org/featured/2020/12/15/openchain-2-1-is-iso5230

Issues for acquiring OpenChain certification (1)

TOYOTA

Issue (1)

I understand the conditions required to obtain certification, but I don't know what to start with.

▼Define the documents required for certification

TOYOTA OpenChain Packages(TOCP)

①	Toyota Open Source General Policy	⑧	OSS Approval List
②	Toyota Open Source Contribution Policy	⑨	OSS Organization Chart
③	Practical Rules for OSS Compliance	⑩	Contribution Check List
④	OSS Compliance Guide Line	⑪	Toyota Open Source Program
⑤	OSS Process	⑫	OpenChain Specification Declaration of certification
⑥	OSS evidence format	⑬	List of roles and capabilities
⑦	OSS Manual	⑭	OSS Program Ability Evidence Document

*Centralize information on the in-house website
Always shared within the organization

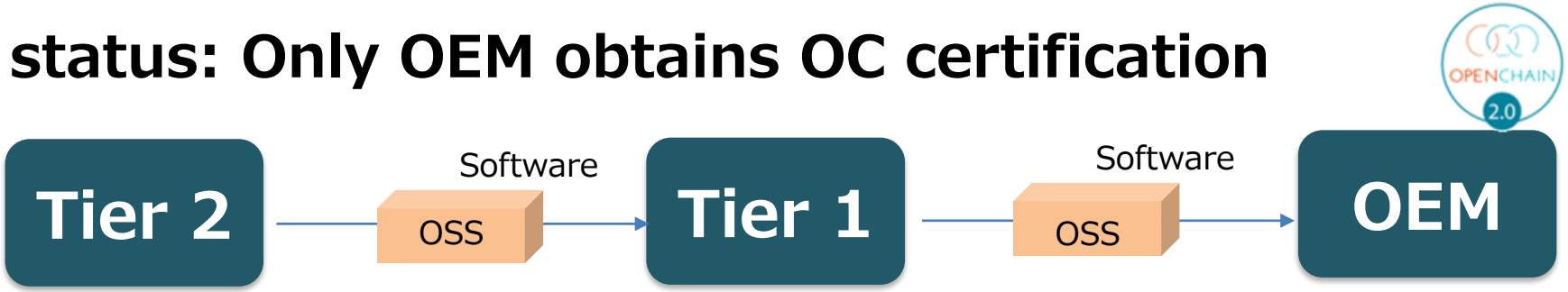
(c)TOYOTA MOTOR CORPORATION 4

https://youtu.be/7DoPe9_yDCk

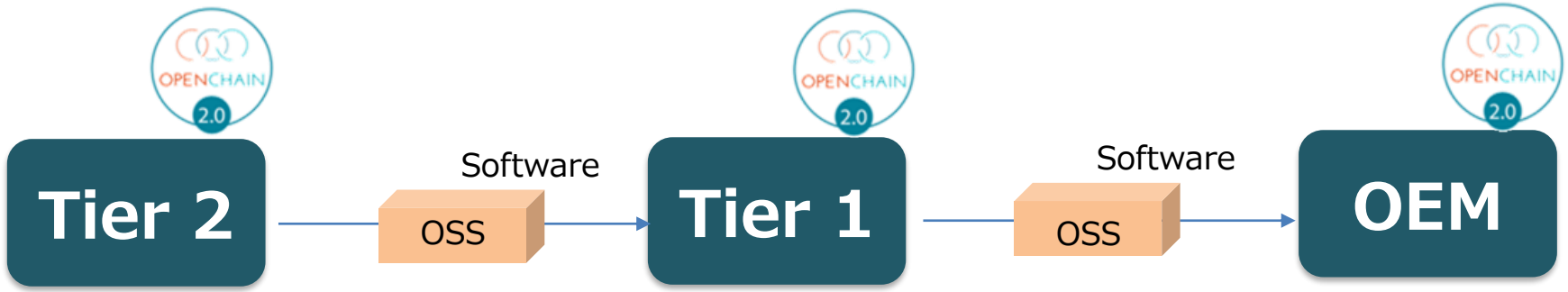
Next Step (1)

▼Promotion of certification acquisition in the automobile industry

Current status: Only OEM obtains OC certification



Aim: All Supply chain companies acquire OC certification



Next Step (2)

▼Promote OpenChain Community

・Disseminate information with the community so that each company can obtain OC certification

・Incorporating practices of Japanese companies and automobile companies

←Automotive Grade Linux (AGL)× OpenChain @ CES2020