FUJITSU

shaping tomorrow with you

Introduction of OpenChain Project

2019.07.02

Agenda

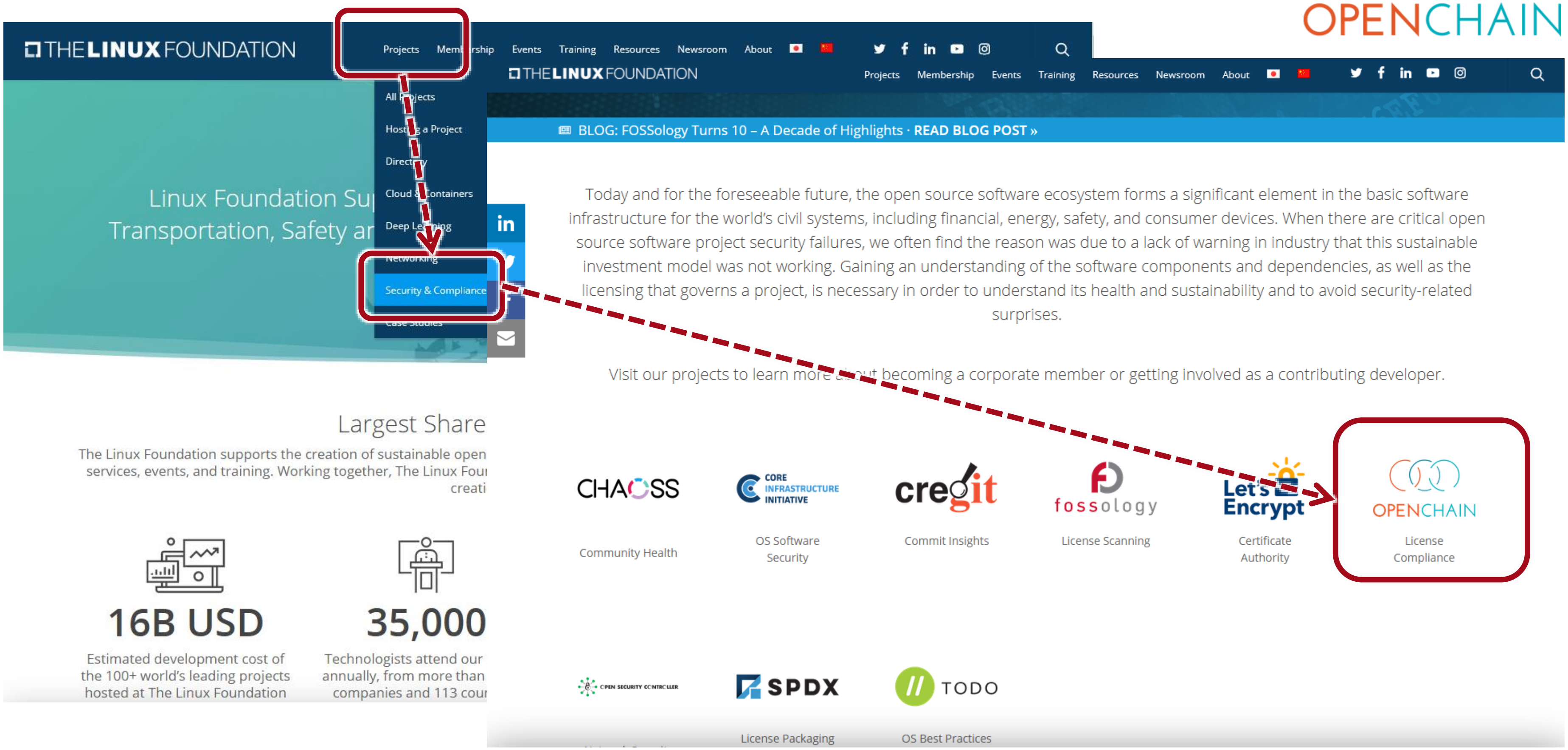
- What’s OpenChain?
- OpenChain Specification
- Activity of Japan Working Group

What’s OpenChain?

OpenChain Project

- OpenChain is the official project of Linux Foundation, which is the largest worldwide OSS community.

OPENCHAIN



THE LINUX FOUNDATION

Projects Membership Events Training Resources Newsroom About

All Projects
Hosting a Project
Directory
Cloud & Containers
Deep Learning
Networking
Security & Compliance
Case Studies

Linux Foundation Su
Transportation, Safety ar

Largest Share

The Linux Foundation supports the creation of sustainable open
services, events, and training. Working together, The Linux Fou
creati

16B USD
Estimated development cost of the 100+ world's leading projects hosted at The Linux Foundation

35,000
Technologists attend our annually, from more than companies and 113 cou

THE LINUX FOUNDATION

Projects Membership Events Training Resources Newsroom About

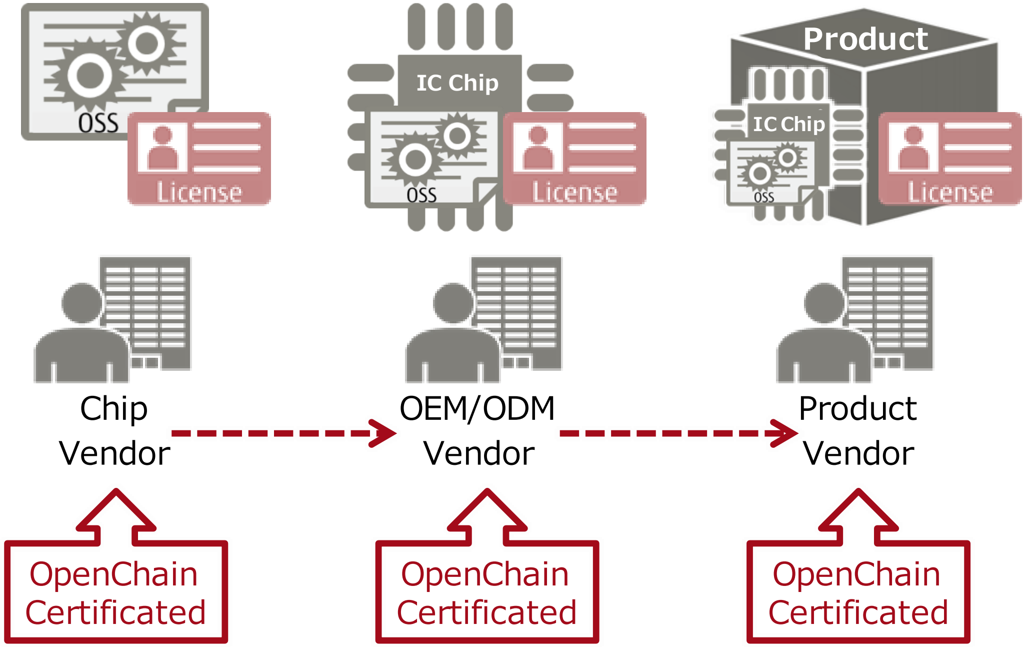
BLOG: FOSSology Turns 10 – A Decade of Highlights · **READ BLOG POST »**

Today and for the foreseeable future, the open source software ecosystem forms a significant element in the basic software infrastructure for the world's civil systems, including financial, energy, safety, and consumer devices. When there are critical open source software project security failures, we often find the reason was due to a lack of warning in industry that this sustainable investment model was not working. Gaining an understanding of the software components and dependencies, as well as the licensing that governs a project, is necessary in order to understand its health and sustainability and to avoid security-related surprises.

Visit our projects to learn more about becoming a corporate member or getting involved as a contributing developer.

Purpose of OpenChain Project

- For build trust across the OSS supply chain, define the requirements of compliance program that organization in supply chain should establish each self as OpenChain specification and promote it.



OSS Supply Chain
(in case of embedded product)

In OpenChain Project, the word “Specification” means “Requirements of compliance program”.

Three pillars of OpenChain Project

- Specification

  Define requirements of compliance program
  that companies should establish within their organization

  ＊Latest Version : 1.2 (in various languages) , Version2.0 (in only English)

- Conformance

  Answering the questions, we can prove compatibility with the above specifications.
  Then, the company name and logo are displayed on the website.

- Curriculum

  A collection of PowerPoint slides for use in in-house educational programs.

OpenChain builds trust across the OSS supply chain by three pillars.
① Define the "Specification"
② Promote many organizations to "Conformance"
③ Provide the "Curriculum"

Platinum Members

- TOYOTA (‘17/8), Hitachi (‘17/9), Sony (‘17/10) joined members of OpenChain.
- Fujitsu has been active since the establishment of the Japan WG, and joined a platinum member in March 2019.

Adobe arm BOSCH cisco COMCAST facebook

FUJITSU Google HITACHI Inspire the Next Microsoft Qualcomm Qualcomm Technologies, Inc. SIEMENS

SONY TOSHIBA TOYOTA Uber Western Digital

Why we joined as a Platinum Member

Significance of platinum member

- □ Avoiding Regal Risk

  As a board member, it is possible to formulate advantageous specifications for Fujitsu.
  Furthermore, improving presence of OSS compliance in supply chain is to avoid legal risks.

- □ Acquisition of competitive advantage

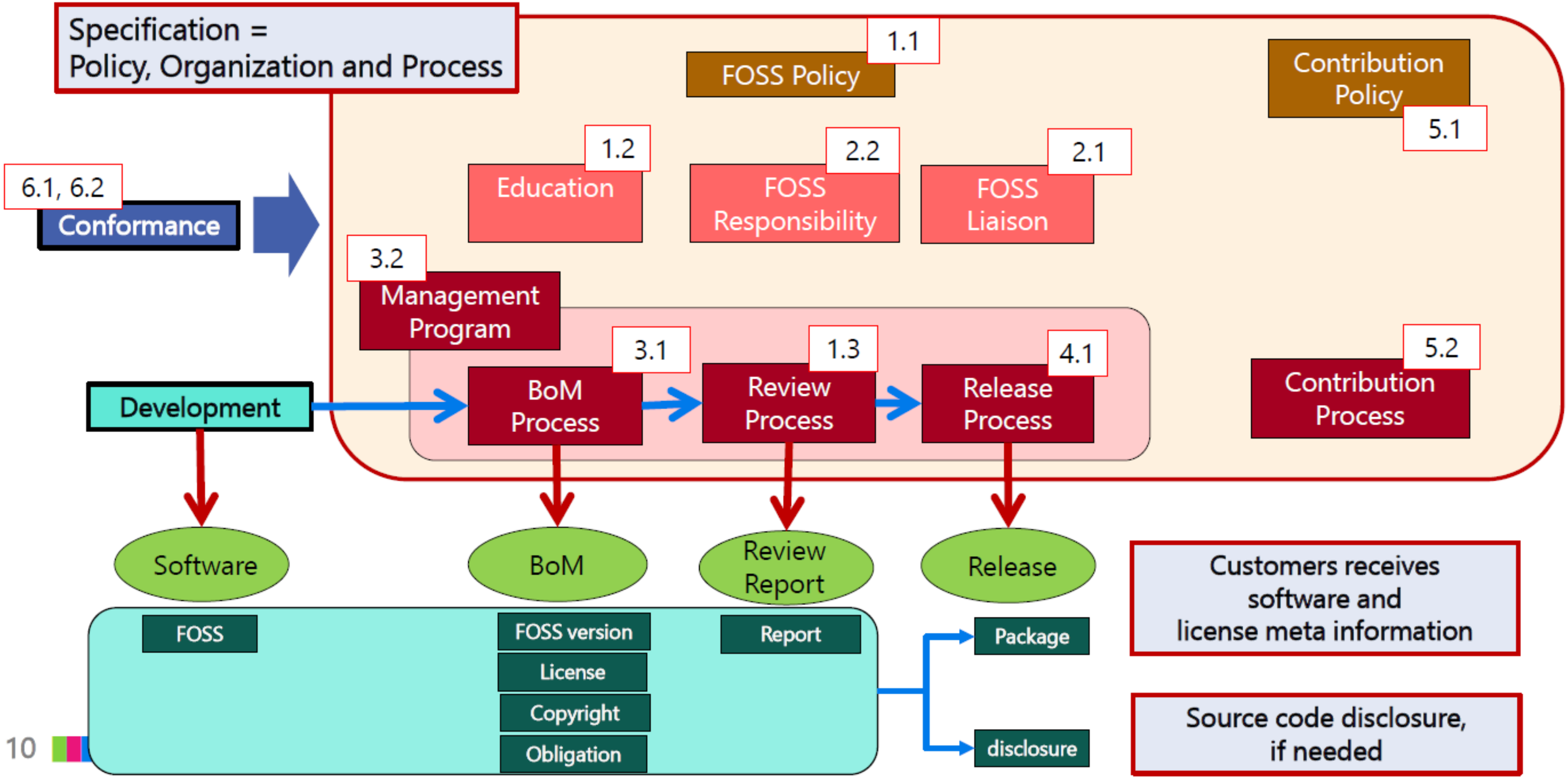
  For example, in the future, customers may only deal with companies that have acquired certification.

By contributing to OpenChain as a platinum member, Fujitsu is enhancing the presence of OSS compliance, leading to advantageous specifications, and working on business revitalization.

OpenChain Specification

Overview of OpenChain Specification

- Define the required specifications according to the process required in the organization.



(*) This image is based on OpenChain ver 1.2.
Now OpenChain ver 2.0 is available (out on April 26, 2019),
and some names of functions are changed.

Definition of requirements

- The items and actions required for each processes are defined in 6 categories.

G1: Know Your FOSS Responsibilities

1.1 A written FOSS policy exists that governs FOSS license compliance of the Supplied Software distribution. The policy must be internally communicated

1.2 Mandatory FOSS training for all Software Staff exists such that:

1.3 A process exists for reviewing the Identified Licenses to determine the obligations, restrictions and rights granted by each license.

G2: Assign Responsibility for Achieving Compliance

2.1 Identify External FOSS Liaison Function.

2.2 Identify Internal FOSS Compliance Role(s).

G3: Review and Approve FOSS Content

3.1 A process exists for creating and managing a FOSS component bill of materials which includes each component (and its Identified Licenses) from which the Supplied Software is comprised.

3.2 The FOSS management program must be capable of handling common FOSS license use cases encountered by Software Staff for Supplied Software, which may include the following use cases:

- distributed in binary form;
- distributed in source form;
- integrated with other FOSS such that it may trigger copyleft obligations;
- contains modified FOSS;
- contains FOSS or other software under an incompatible license interacting with other components within the Supplied Software; and/or
- contains FOSS with attribution requirements.

Definition of requirements

- The items and actions required for each processes are defined in 6 categories.

G4: Deliver FOSS Content Documentation and Artifacts

4.1 A process exists for creating the set of Compliance Artifacts for each Supplied Software release.
- source code, notice, copyright, copy of license, SPDX documents, etc.

G5: Understand FOSS Community Engagement

5.1 A written policy exists that governs contributions to FOSS projects by the organization. The policy must be internally communicated.

5.2 If an organization permits contributions to FOSS projects then a process exists that implements the FOSS contribution policy outlined in Section 5.1.

G6: Certify Adherence to OpenChain Requirements

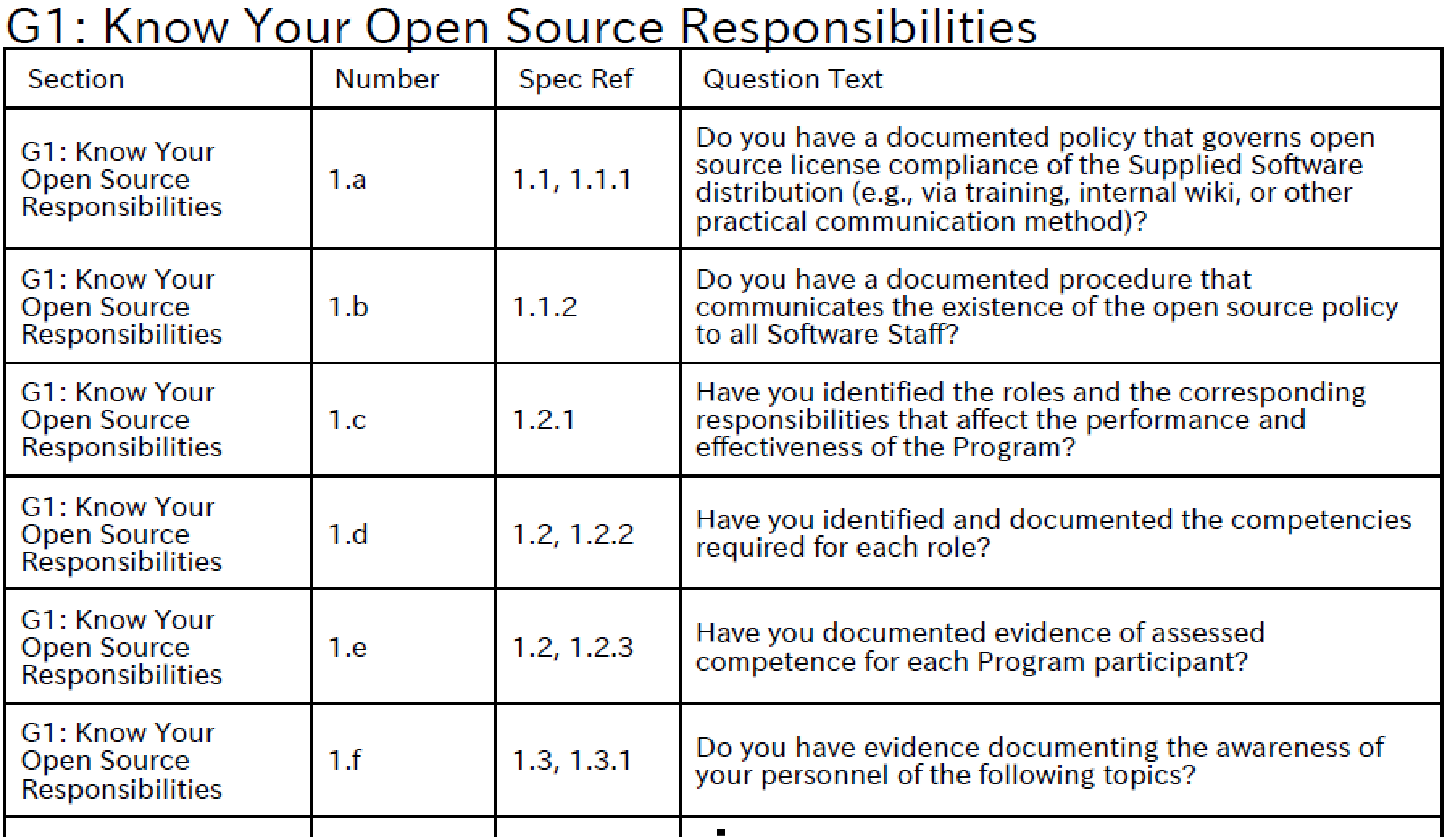
6.1 In order for an organization to be OpenChain Certified, it must affirm that it has a FOSS management program that meets the criteria described in this OpenChain Specification version 1.2.

6.2 Conformance with this version of the specification will last 18months from the date conformance validation was achieved. Conformance validation requirements can be found on the OpenChain project's website.

Self-Certification

FUJITSU

- Publish the self-checklist to measure the conformance to the OpenChain specification.



G1: Know Your Open Source Responsibilities

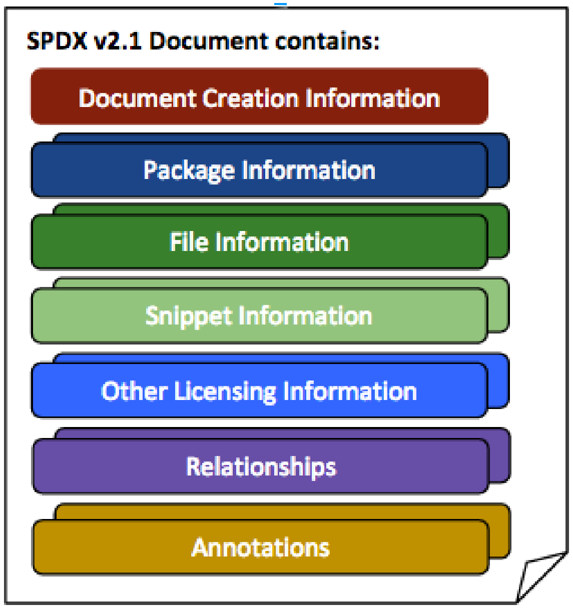
Section	Number	Spec Ref	Question Text
G1: Know Your Open Source Responsibilities	1.a	1.1, 1.1.1	Do you have a documented policy that governs open source license compliance of the Supplied Software distribution (e.g., via training, internal wiki, or other practical communication method)?
G1: Know Your Open Source Responsibilities	1.b	1.1.2	Do you have a documented procedure that communicates the existence of the open source policy to all Software Staff?
G1: Know Your Open Source Responsibilities	1.c	1.2.1	Have you identified the roles and the corresponding responsibilities that affect the performance and effectiveness of the Program?
G1: Know Your Open Source Responsibilities	1.d	1.2, 1.2.2	Have you identified and documented the competencies required for each role?
G1: Know Your Open Source Responsibilities	1.e	1.2, 1.2.3	Have you documented evidence of assessed competence for each Program participant?
G1: Know Your Open Source Responsibilities	1.f	1.3, 1.3.1	Do you have evidence documenting the awareness of your personnel of the following topics?

⋮

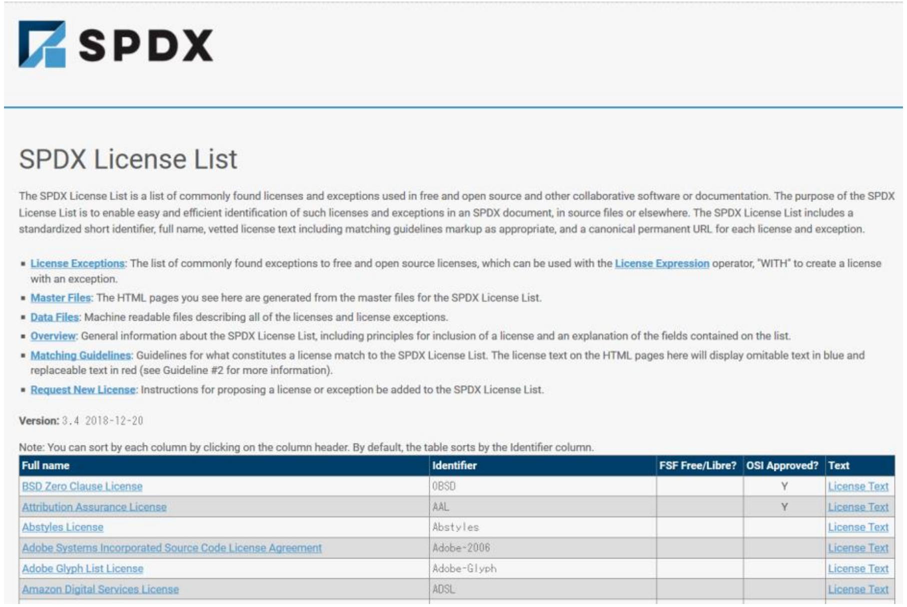
SPDX Format

- SPDX stands for “Software Package Data eXchange”
  - The specification for exchange software package information standardized and published by Linux Foundation.
  - It includes the information about license, copyright, and so on.
- To make the SPDX format document, we can use the tool “FOSSology” published by Linux Foundation.
  - FOSSology can check about 500 kinds of license.

fossology



SPDX v2.1 Document contains:
Document Creation Information
Package Information
File Information
Snippet Information
Other Licensing Information
Relationships
Annotations



SPDX

SPDX License List

The SPDX License List is a list of commonly found licenses and exceptions used in free and open source and other collaborative software or documentation. The purpose of the SPDX License List is to enable easy and efficient identification of such licenses and exceptions in an SPDX document, in source files or elsewhere. The SPDX License List includes a standardized short identifier, full name, vetted license text including matching guidelines markup as appropriate, and a canonical permanent URL for each license and exception.

- License Exceptions: The list of commonly found exceptions to free and open source licenses, which can be used with the License Expression operator, "WITH" to create a license with an exception.
- Master Files: The HTML pages you see here are generated from the master files for the SPDX License List.
- Data Files: Machine readable files describing all of the licenses and license exceptions.
- Overview: General information about the SPDX License List, including principles for inclusion of a license and an explanation of the fields contained on the list.
- Matching Guidelines: Guidelines for what constitutes a license match to the SPDX License List. The license text on the HTML pages here will display omitable text in blue and replaceable text in red (see Guideline #2 for more information).
- Request New License: Instructions for proposing a license or exception be added to the SPDX License List.

Version: 3.4 2018-12-20

Note: You can sort by each column by clicking on the column header. By default, the table sorts by the Identifier column.

Full name	Identifier	FSF Free/Libre?	OSI Approved?	Text
BSD Zero Clause License	0BSD		Y	License Text
Attribution Assurance License	AAL		Y	License Text
Abstyles License	Abstyles			License Text
Adobe Systems Incorporated Source Code License Agreement	Adobe-2006			License Text
Adobe Glyph List License	Adobe-Glyph			License Text
Amazon Digital Services License	ADSL			License Text

Ex. File Information

FUJITSU

License and copyright information in each files

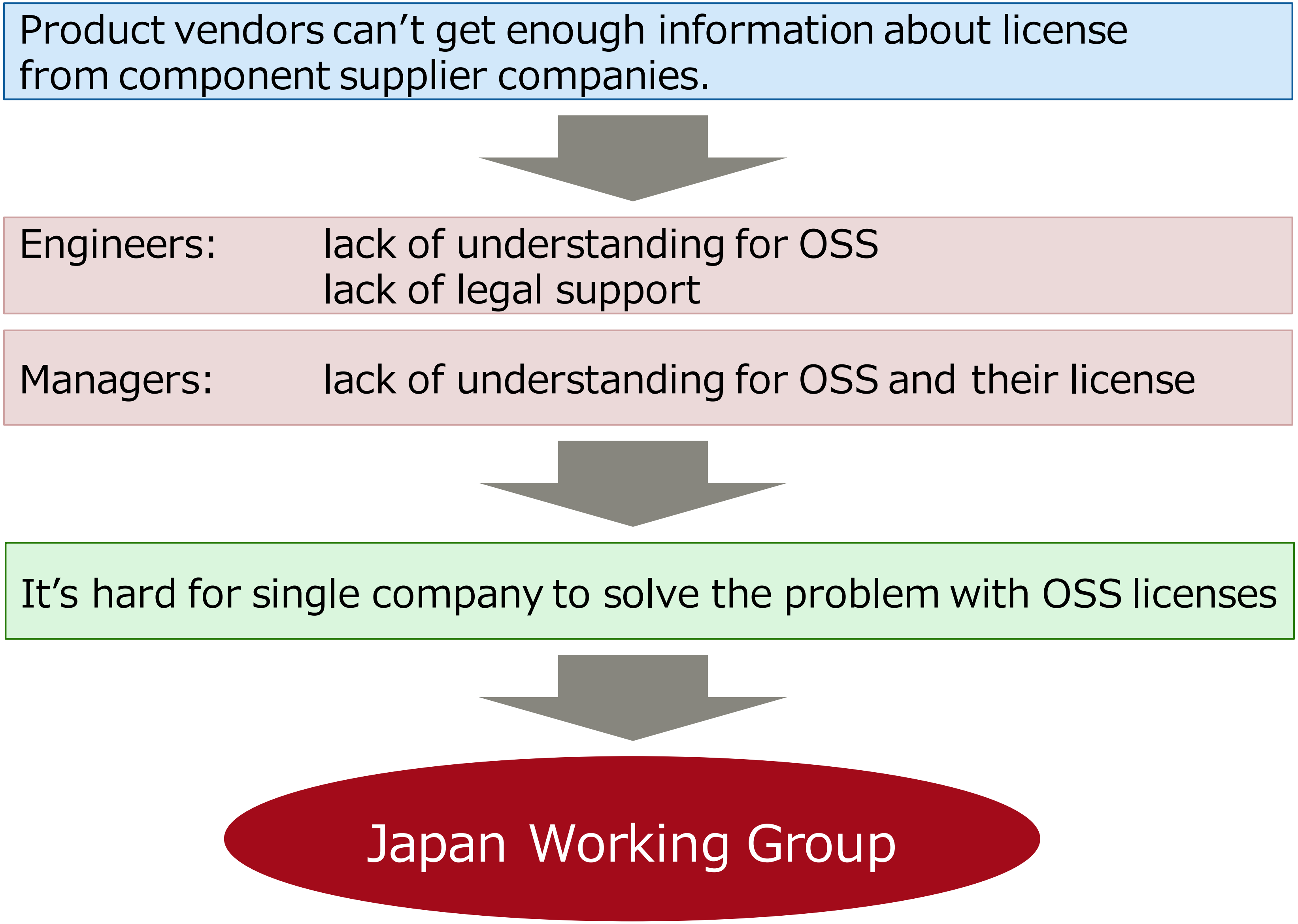
- File Name:
  name of the file and its path
- License Information:
  declared license found in the file
- FileCopyrightText:
  copyright holder and its date

```
##File

FileName: spdx_temp/hostapd-2.6/COPYING
SPDXID: SPDXRef-item584869
FileChecksum: SHA1: xxxx
FileChecksum: MD5:xxxx
LicenseConcluded: NOASSERTION
LicenseInfoInFile: GPL-2.0
FileCopyrightText: NOASSERTION
```

```
##File

FileName: tmpqslhxvgf/git/ubi-utils/ubidetach.c
SPDXID: SPDXRef-item938
FileChecksum: SHA1: xxxx
FileChecksum: MD5: xxxx
LicenseConcluded: NOASSERTION
LicenseInfoInFile: GPL-2.0
FileCopyrightText: <text>
Copyright (C) 2007 Nokia Corporation. </text>
```

Activity of Japan Working Group

The problem with OSS in Japan



Product vendors can’t get enough information about license from component supplier companies.

Engineers: lack of understanding for OSS
lack of legal support

Managers: lack of understanding for OSS and their license

It’s hard for single company to solve the problem with OSS licenses

Japan Working Group

OpenChain Japan WG

- Mission:
  - Making environment for engineers in Japan and Asian countries to use OSS appropriately

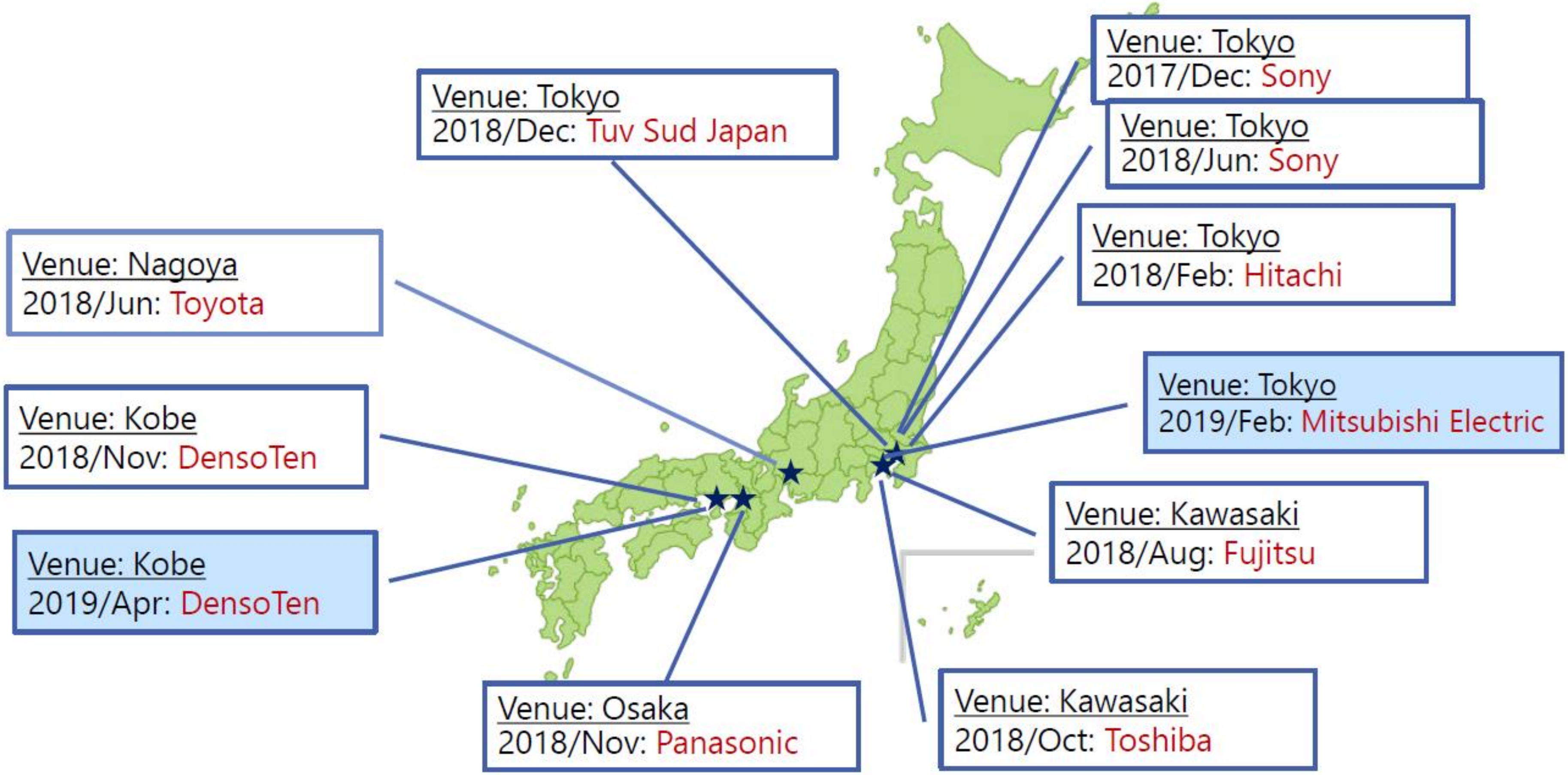
- Activities:
  - Solving problem in Japan
  - Promoting OSS compliance in Japan and Asian countries
  - Exchanging information about OSS license

OpenChain Japan WG Sub Groups

- **Planning Sub Group**
  - ➡ Team Lead: Hiroyuki Fukuchi (Sony)
- **FAQ Sub Group**
  - ➡ Team Lead: Yoshiko Ohuchi (Fujitsu)
- **Leaflet Sub Group**
  - ➡ Team Lead: Osamu Ueda (Sony)
- **Education Materials Sub Group**
  - ➡ Team Lead: Yoshitaka Iwata (Hitachi)
- **Exchanging License Information Sub Group** * Planning SPDX Lite version
  - ➡ Team Lead: Yoshiyuki Itoh (Renesus Electronics)
- **Tool Sub Group** * Implementing SPDX Lite version
  - ➡ Team Lead: Yoshitake Kobayashi (Toshiba)
- **Promotion Sub Group**
  - ➡ Team Lead: Masato Endo (TOYOTA)

OpenChain Japan WG Meetings

- Participating companies take turns to provide meeting place each meeting (every 2-3 months).



Venue: Tokyo
2017/Dec: Sony

Venue: Tokyo
2018/Feb: Hitachi

Venue: Tokyo
2018/Jun: Sony

Venue: Nagoya
2018/Jun: Toyota

Venue: Kawasaki
2018/Aug: Fujitsu

Venue: Kawasaki
2018/Oct: Toshiba

Venue: Kobe
2018/Nov: DensoTen

Venue: Osaka
2018/Nov: Panasonic

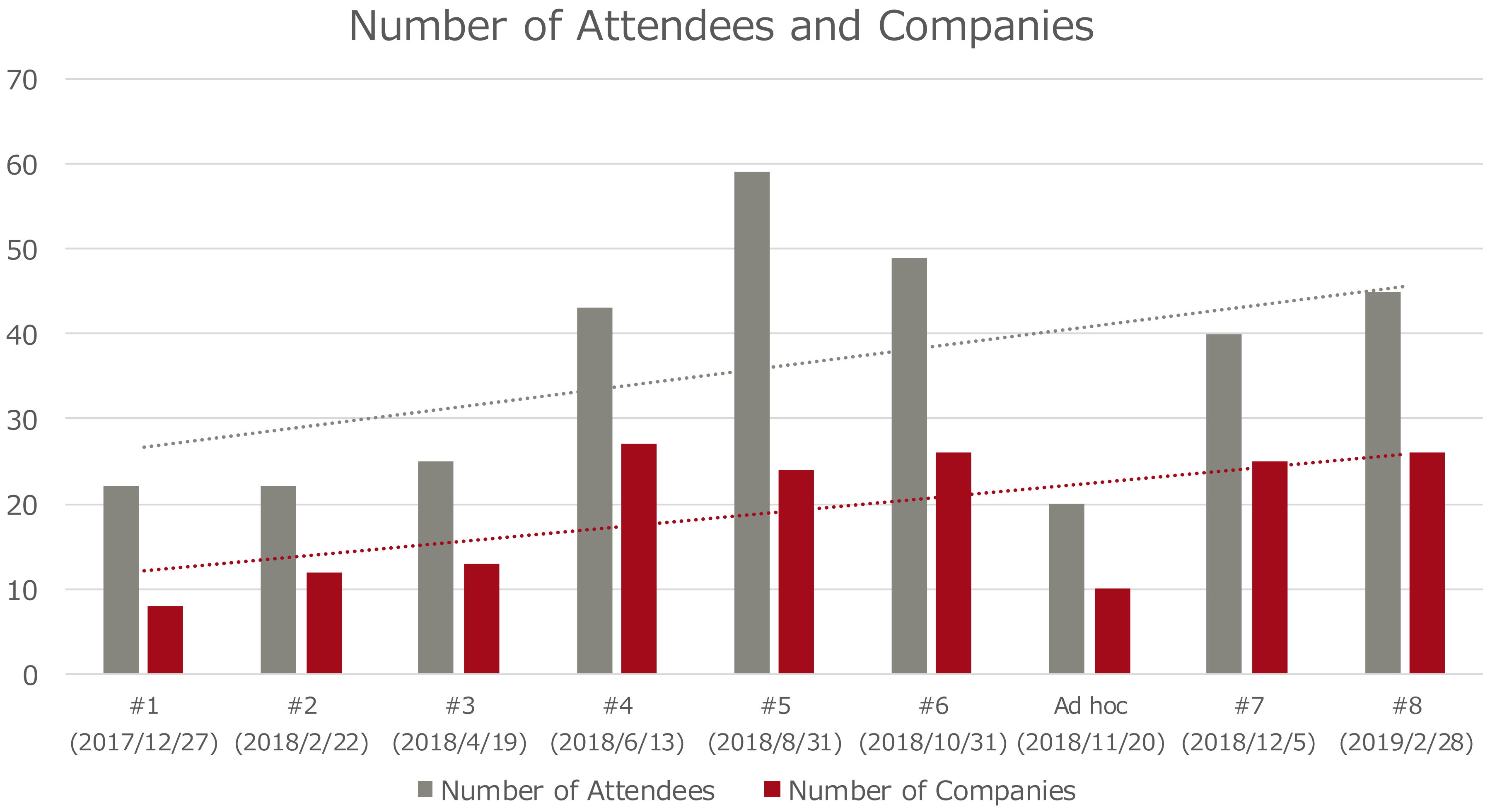
Venue: Tokyo
2018/Dec: Tuv Sud Japan

Venue: Tokyo
2019/Feb: Mitsubishi Electric

Venue: Kobe
2019/Apr: DensoTen

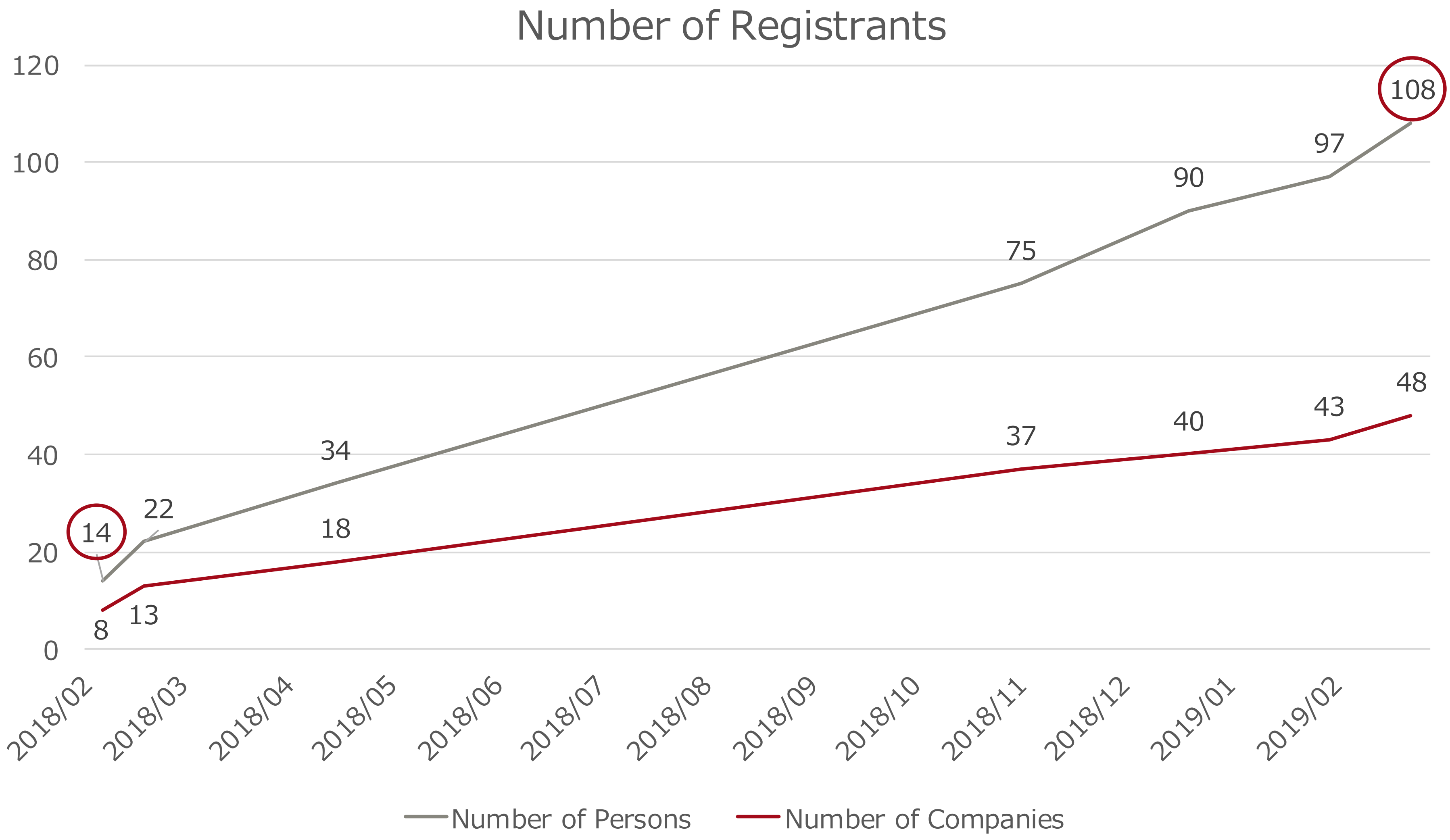
Meetings in Japan

- Number of attendees and companies is increasing every meetings.



Japan ML registrants

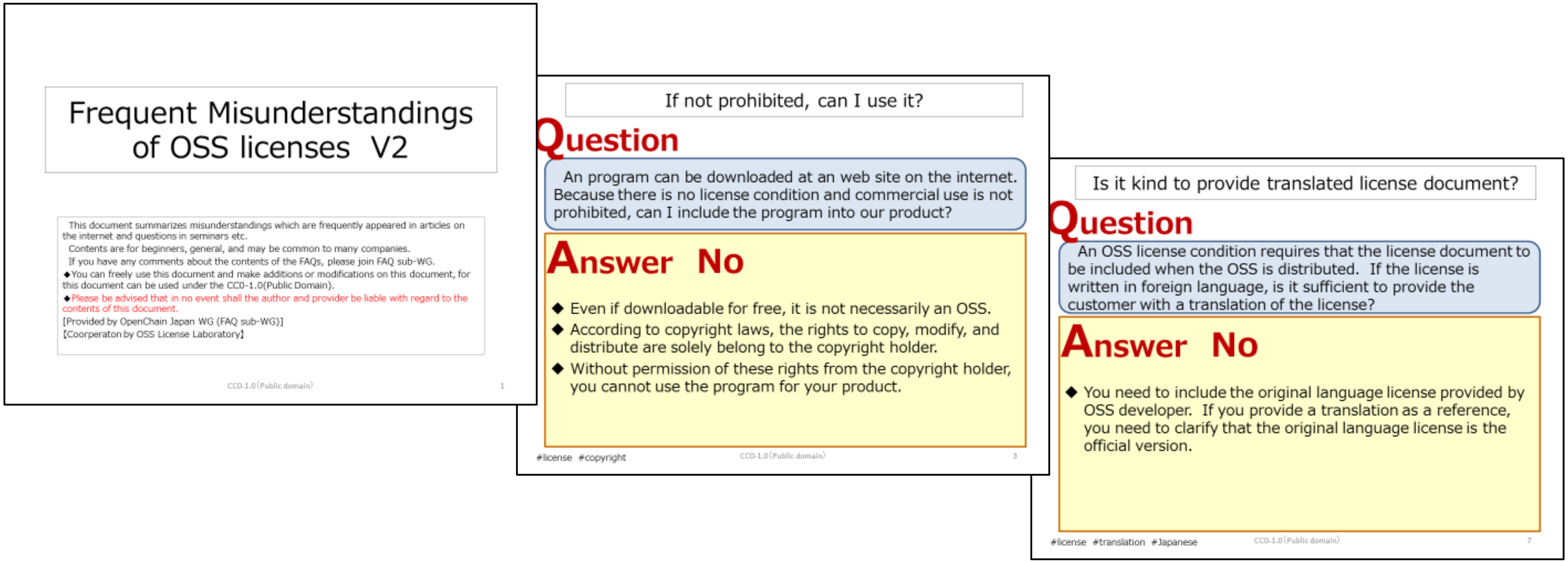
- Number of registrants is constantly increasing.



Outcomes of Japan WG

- Publish FAQ for OSS Licenses
  - English and Japanese versions are available at GitHub

https://github.com/OpenChain-Project/Onboarding-JWG/blob/master/Education_Material/FAQ



Frequent Misunderstandings of OSS licenses V2

This document summarizes misunderstandings which are frequently appeared in articles on the internet and questions in seminars etc.

Contents are for beginners, general, and may be common to many companies.

If you have any comments about the contents of the FAQs, please join FAQ sub-WG.

◆You can freely use this document and make additions or modifications on this document, for this document can be used under the CC0-1.0(Public Domain).

◆Please be advised that in no event shall the author and provider be liable with regard to the contents of this document.

[Provided by OpenChain Japan WG (FAQ sub-WG)]

【Coorperaton by OSS License Laboratory】

CC0-1.0（Public domain） 1

If not prohibited, can I use it?

Question

An program can be downloaded at an web site on the internet. Because there is no license condition and commercial use is not prohibited, can I include the program into our product?

Answer No

◆ Even if downloadable for free, it is not necessarily an OSS.

◆ According to copyright laws, the rights to copy, modify, and distribute are solely belong to the copyright holder.

◆ Without permission of these rights from the copyright holder, you cannot use the program for your product.

#license #copyright CC0-1.0（Public domain） 3

Is it kind to provide translated license document?

Question

An OSS license condition requires that the license document to be included when the OSS is distributed. If the license is written in foreign language, is it sufficient to provide the customer with a translation of the license?

Answer No

◆ You need to include the original language license provided by OSS developer. If you provide a translation as a reference, you need to clarify that the original language license is the official version.

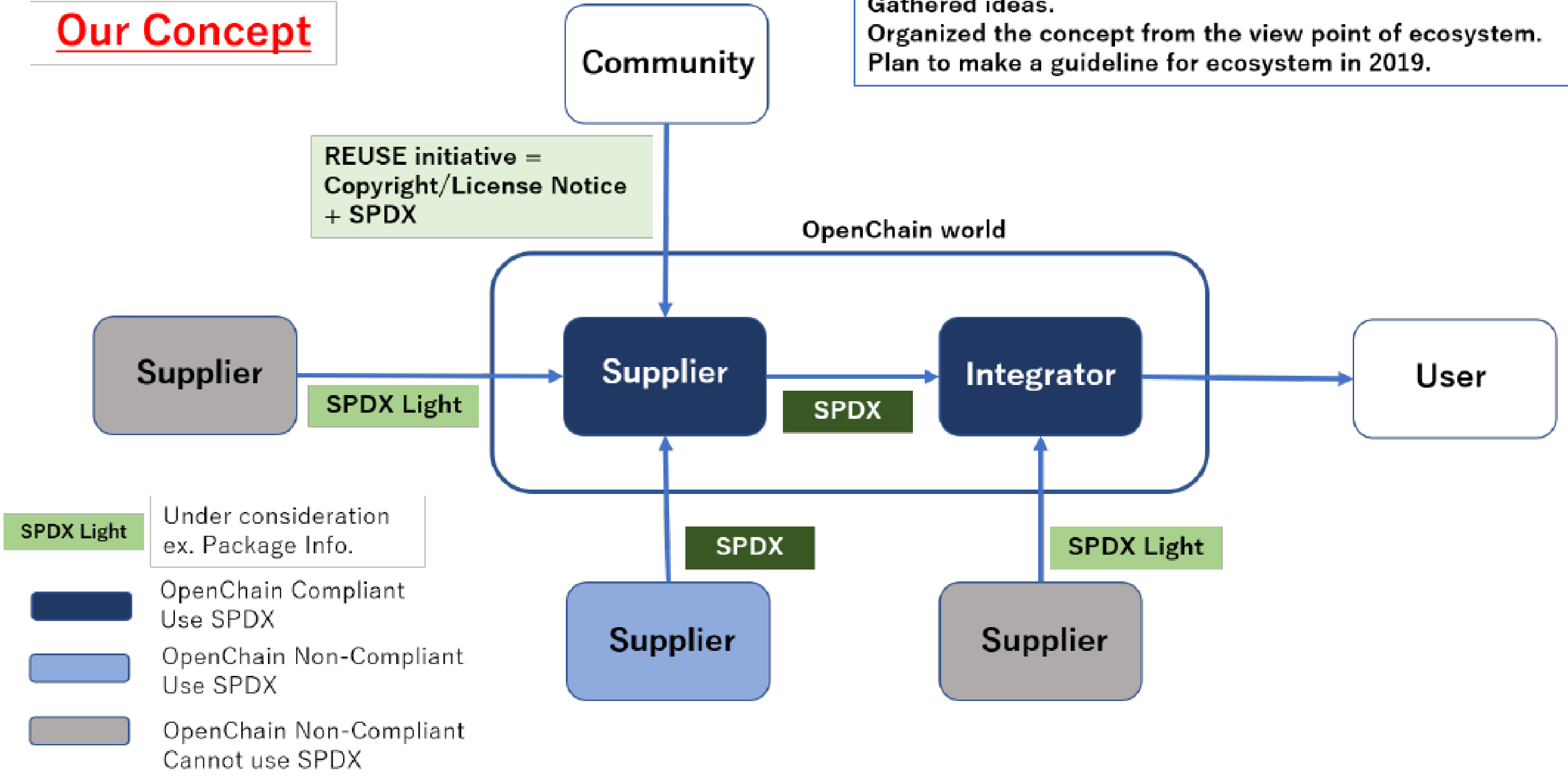
#license #translation #Japanese CC0-1.0（Public domain） 7

Outcomes of Japan WG

Guideline for Exchanging License Info (Under Discussion)

Status:
Gathered ideas.
Organized the concept from the view point of ecosystem.
Plan to make a guideline for ecosystem in 2019.

Our Concept



How to Join OpenChain

- OpenChain Website https://www.openchainproject.org/
- OpenChain Wiki https://wiki.linuxfoundation.org/openchain/
  - Japan WG Wiki https://wiki.linuxfoundation.org/openchain/openchain-japanese-working-group
- Mailing Lists
  - Main Mailing List
  - Specification Mailing List
  - Curriculum Mailing List
  - Conformance Mailing List
  - Japan WG Mailing List openchain-japan-wg@lists.linuxfoundation.org
- Teleconference
  - First Tuesday, 2:00 AM JST (1h advance when summer time in the US)
  - Third Tuesday, 10:00 AM JST (1h advance when summer time in the US)

FUJITSU

shaping tomorrow with you