SPDX Light
material for discussion with SPDX team

Hiroyuki Fukuchi

Overview of activity by Japan WG

- Issues recognized in Japan WG
  - License Info. between organizations
  - Insufficient copyright notice written by a community developer

- Starting sub group
  - Case study and proposal
  - License info. based on SPDX
  - SPDX light
    - Current status (case study, candidate)
    - Plan for future (explanation, examples, procedure to make, tooling)
  - REUSE initiatives

- Promotion of SPDX
  - Document for beginners
  - Tooling

Issues of license info.

- Appropriate license info. is not provided by suppliers.
  - Some suppliers do not know OSS license.
  - (Knowledge)

  - Other suppliers indirectly refuse to provide license info..
  - (Workload)
    - “I do not know OSS license…”
    - “Only your company requests such info…”

  - Different customers ask different formats.
  - (No Standard)
    - In automotive industry, a supplier has many customer companies.

Issues of copyright notice

- Background
  - Companies want to do internal compliance process automatically by tools.

- Copyright notice is not at all written in the source code from upper stream.
- (Knowledge)

- Copyright is written, but in the different ways in each source code.
- (No Standard)
  - There are too many patterns to scan automatically by tools.
  - So engineers do compliance tasks, instead of development.
  -

Discussion in Japan WG #1

- It is nice to make a guideline for exchanging license info. including copyright notice.
  - Exchanging license info. between organization is out of scope of the OpenChain.
  - Guideline does not give rules that a company must comply with.
  - Guideline is a good way to show an appropriate procedure.

- There is the SPDX, we should use the standard.
  - Reinvention is not good.
  - Intermittent suppliers in the supply chain like semiconductor companies have to hold all the information.
  - If an intermittent supplier lose information, a company in down stream cannot recover it.
  - Renesas and Fujitsu are using the SPDX.

Discussion in Japan WG #2

- However, in the supply chain, there are many small companies that cannot make an SPDX file by themselves.
  - SPDX specification is not broadly known by engineers.
  - Making an SPDX file requires to use compliance tools.
  - In some cases, the size of an SPDX file is very huge due to “RELATIONSHIP”.

- SPDX light has been discussed in subgroup of Japan WG.
  - Should be easy to understand
  - Should be easy to make
  - Should have enough information to comply with OSS license
  - Should have the affinity with SPDX, that means the subset of SPDX.

Discussion in Japan WG #3

- REUSE initiative gives us the good path to access OSS communities
  - It recommends a standard to write copyright notice and license notice.
  - Standardization of notice is good for machine to do compliance process.
  - It also recommends SPDX.
  - Japan WG does not have the appropriate paths to OSS communities, but REUSE initiative can access broadly.
  - Of course, SPDX is!!

- We think SPDX and SPDX light can cover all the supply chain.

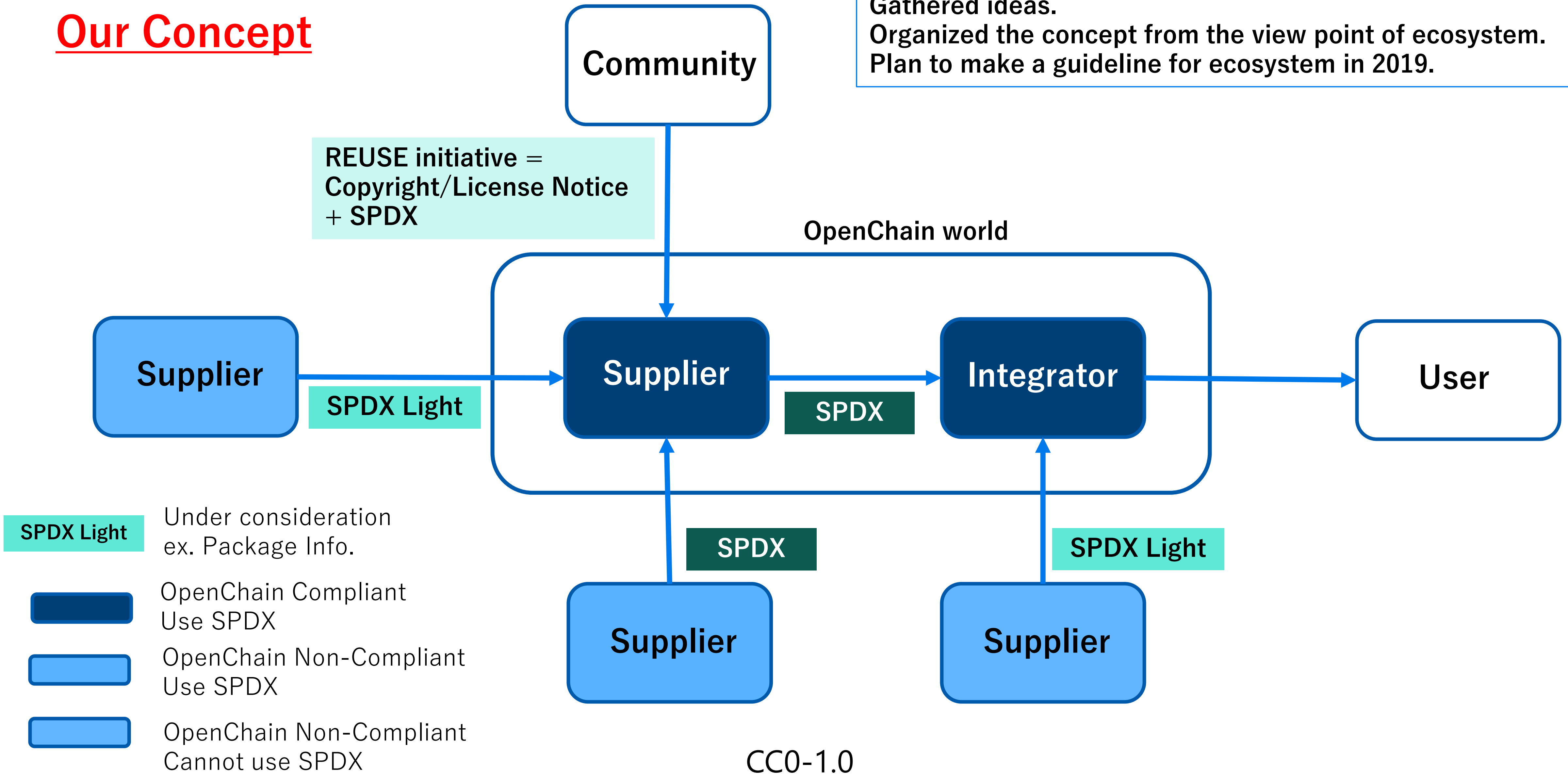
- SPDX light is the entry point to the SPDX world.
  - We hope entry users change their format from SPDX light to SPDX.

OpenChain Japan WG

Guideline for Exchanging License Info.

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

Our Concept



SPDX Light — Under consideration ex. Package Info.

■ OpenChain Compliant Use SPDX

▭ OpenChain Non-Compliant Use SPDX

▭ OpenChain Non-Compliant Cannot use SPDX

SPDX light

- Case study on actually used list.
- Almost items are included in Package Information

- Candidate is created by the lists that are actually used in business.

Further consideration

- SPDX is designed to carry the information from upper stream to down stream. (Downward)

- Some companies including OEM companies want to manage software in the supply chain.
  - A company's policy may not allow to use copyleft license.
- This means that an entity in down stream want to manage the stream(the supply chain). (Upward)

- It is useful for business to define an additional file besides the SPDX file. (ongoing)

Items of SPDX light (draft)

SPDX version 2.1	License Info.	Rationale
3.1 Package Name	Software Name	To identify software
3.3 Package Version	Version	To identify specific version
3.4 Package File Name	Package File Name	To identify specific package
3.7 Package Download Location	Source Code Download Location URL	To get the same software
3.11 Package Home Page	Project Website URL	To verify relevant information
3.13 Concluded License	License	
3.15 Declared License	License	
3.16 Comments on License	Comments on License	To verify additional conditions
3.17 Copyright Text	Copyright Text	
3.22 External reference comment	Modification record	
6.1 License Identifier, 6.2 Extracted Text 6.3 License Name 6.5 License Comment	Additional Info.	To specify licenses which are not on the SPDX license list / To specify dual license

https://github.com/OpenChain-Project/Japan-WG-General/blob/master/License-Info-Exchange/Doc-at-Meeting/Candidate-of-SDPX-light.md

Plan for future (SPDX light)

- Examples for model cases
- Procedure to make SPDX light file
- Explanation of SPDX light
- Tooling for SPDX

An idea for SPDX promotion
Comprehensive explanation of SPDX by Kate Stewart

- Chapter 11 SOFTWARE PACKAGE DATA EXCHANGE® (SPDX®)
- INTRODUCTION
  - SPDX License List
  - SPDX License IDs
  - SPDX Specification – Background
  - Overview of an SPDX Document
  - Document Creation Information
  - Package Information
  - File Information
  - Snippet Information
  - Other Licensing Information
  - Relationships
  - Annotations
  - Tools and Other Resources for Sharing SPDX Documents
  - Tools That Can Generate SPDX Documents
  - Tools Able to Import SPDX Documents
  - Help Improve SPDX 173

Open Source Compliance in the enterprize
By Ibrahim Haddad, Shane Coughlan, Kate Stewart

https://www.linuxfoundation.jp/blog/2018/12/new-ebook-offers-comprehensive-guide-to-open-source-compliance/

Resources

- OpenChain project:
  - Website: https://www.openchainproject.org/
  - Wiki: https://wiki.linuxfoundation.org/openchain/start
  - GitHub: https://github.com/OpenChain-Project
  - ML: openchain@lists.linuxfoundation.org
  - Translations: https://www.openchainproject.org/translations

- OpenChain Japan WG:
  - Wiki: https://wiki.linuxfoundation.org/openchain/openchain-japanese-working-group
  - ML: openchain-japan-wg@lists.linuxfoundation.org
  - GitHub: https://github.com/OpenChain-Project/Onboarding-JWG
  - https://github.com/OpenChain-Project/Japan-WG-General

- SPDX:
  - Website: https://spdx.org/

- SPDX 2.1 非公式日本語訳
  - GitHub: https://github.com/hfukuchi/SPDX_specification/tree/master/chapters