

OpenChain Japan Work Group Tooling Sub-Group

Speaker: Takashi NINJOUJI
Q&A mgt., Demo : Kouki HAMA

OpenChain Japan WG / Tooling SG
2020/04/23

Tooling SG の目的

OSS管理運用のためのOSS(ツール)を利用して、
Open Source Compliance において次を実現する

1. 組織に応じたワークフローの構築
2. 省力化 (オートメーション)
3. 質の向上 (ツール、ワークフロー、コンプライアンスについて)

Tooling SG の活動内容

日本語中心でOK

- 1. ツールの情報をまとめる / 発信する**
(Globalコミュニティと連携)
- 2. 実際に使いながら勉強や議論する場の提供**
(ツール紹介、セミナーやハンズオンの開催など)
- 3. 情報流通とツールのマッピング**
(ワークフロー実現のために課題を洗い出し、他と連携して改善)
- 4. 活動に賛同するメンバ拡大のためのプロモーション**
(OpenChain以外の会合での発表、Githubやその他メディアの活用)

関連する主なコミュニティ



国内外に仲間がいます

1. OpenChain Reference Tooling Work Group, 開発コミュニティ

(<https://github.com/Open-Source-Compliance/Sharing-creates-value>)

(FOSSology: <https://www.fossology.org>)

(SW360: <https://projects.eclipse.org/projects/technology.sw360>)

(OSS Review Toolkit: <https://oss-review-toolkit.org/>)

2. OpenChain Japan-WG, ライセンス情報SG

(<https://openchain-project.github.io/OpenChain-JWG/subgroups/licensing/>)

3. SPDX Workgroup

(<https://spdx.org>)

4. これから開拓するかも : ToDo Group

(<https://todogroup.org>)

Tooling SGの情報や参加方法



日本語中心でOK

1. Github

(<https://openchain-project.github.io/OpenChain-JWG/subgroups/tooling/>)

2. メーリングリスト

(<https://lists.openchainproject.org/g/japan-sg-tooling/>)

3. Slack #tooling-sg

(<https://openchain-japanwg.slack.com/archives/CGHP86Y4T>)

4. 会合

(1-2ヶ月に一度の開催)

Tooling SG : 2019年度 活動概要



日時	実施内容	参加
第1回 2019/3/13	<ul style="list-style-type: none"> CFP確認と今後の活動方針についての議論 	7社 14名
第2回 2019/4/25	<ul style="list-style-type: none"> SPDX Toolsの紹介 コンプライアンス管理ツールSW360 OpenChain Tooling WG活動状況紹介 	16社 28名
第3回 2019/6/20	<ul style="list-style-type: none"> OpenChain仕様を考慮したSW360の運用 Brief Introduction into ClearlyDefined FOSSologyのCLI / REST APIを叩いてみた 	11社 19名
第4回 2019/8/29	<ul style="list-style-type: none"> ライセンス読み解き情報について OpenChain Global Tooling WG立ち上げ OSSNA参加報告 	10社 19名
第5回 2019/10/17	<ul style="list-style-type: none"> FOSSology - Install from Source ScanTool Comparison 	7社 17名
第6回 2019/12/19	<ul style="list-style-type: none"> SW360 Workshop <p>Speaker: Michael C. Jaeger from Siemens Co-Maintaining FOSSology and SW360</p>	19社 36名
Special 2019/12/20	<ul style="list-style-type: none"> FOSSology Workshop <p>Speaker: Michael C. Jaeger from Siemens Co-Maintaining FOSSology and SW360</p>	16社 33名
第7回 2020/2/17 (オンライン開催)	<ul style="list-style-type: none"> CHAOSS紹介 Managing OSS Vulnerability w/ Software Component Catalogue, SW360 Automotive WGで発表したsw360,FOSSology, SPDX Lite SPDX Liteと現状のtoolのギャップ Open Chain reference tooling wg f2f mtg 参加報告 	17社 31名

Tooling SG : 次回会合の案内



日時 : 2020年5月20日(水) 10:00-12:00

場所 : オンライン開催

お題 : 自由

- 発表者を募集します！
- 発表申込手順等、メーリングリストとSlackで案内予定

※今後の運営についても、メーリングリストやSlackで議論しましょう

(次回に向けて、ただいま準備中)



(OSS Review Toolkit を試しています...)

Breaking News!



1. SW360 更新情報

a. 多言語化サポート！

a. <https://github.com/eclipse/sw360/releases/tag/sw360-8.2.0-M1>

2. 日本語訳のレビューを募集！

a. https://github.com/KoukiHama/sw360/blob/addJapanese/frontend/sw360-portlet/src/main/resources/content/Language_ja.properties

Tooling コミュニティ及び関連の動向



1. ツールのプラガビリティ

- a. REST API の拡充
- b. SPDX のサポート

2. コンテナ

- a. ソースアーティファクトの関連付け、そのSBOMの作成と配布方法
 - i. OCI (Open Container Initiative) でイメージとの関連付けについて議論がある

3. セキュリティ: SBOMと脆弱性管理

- a. SBOM Format: SPDX, SWID (ISO/IEC 19770-2), CycloneDX (OWASP)
- b. Cyber Security, C-SCRM, DevSecOps, dependency

ありがとうございました



【再掲】

Tooling SG : 次回会合の案内

日時 : 2020年5月20日(水) 10:00-12:00

場所 : オンライン開催

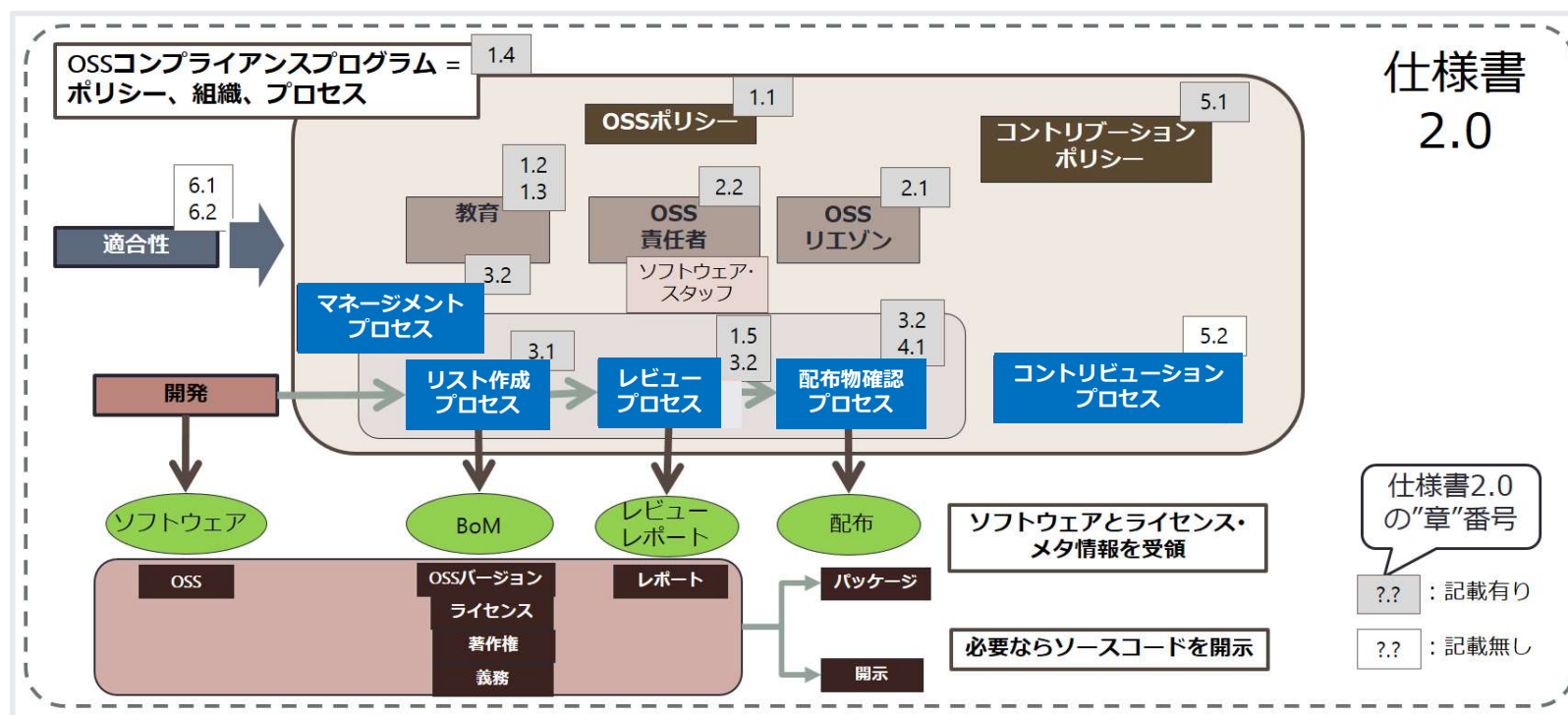
お題 : 自由

- 発表者を募集します！
- 発表申込手順等、メーリングリストとSlackで案内予定

次以降のスライドは、時間があまった場合

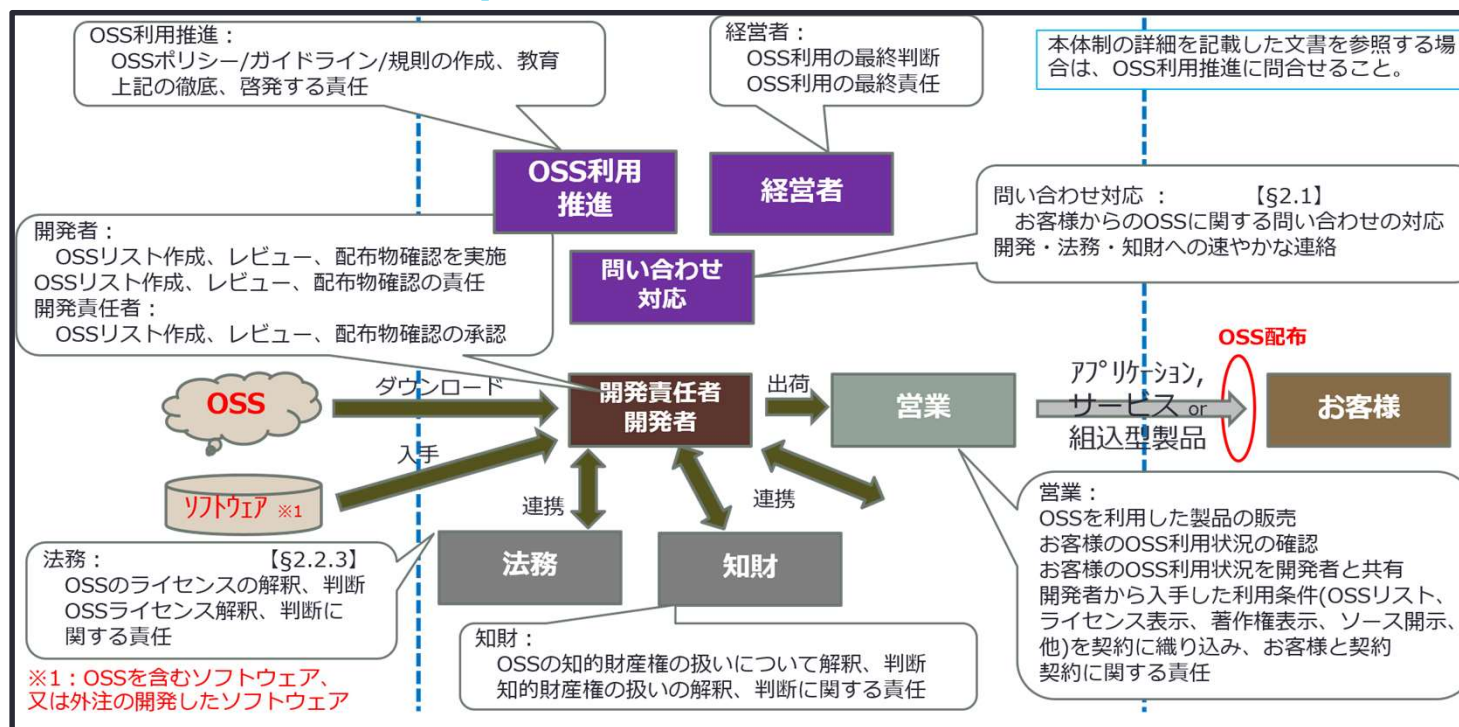


OpenChain Specification 2.0 の概観



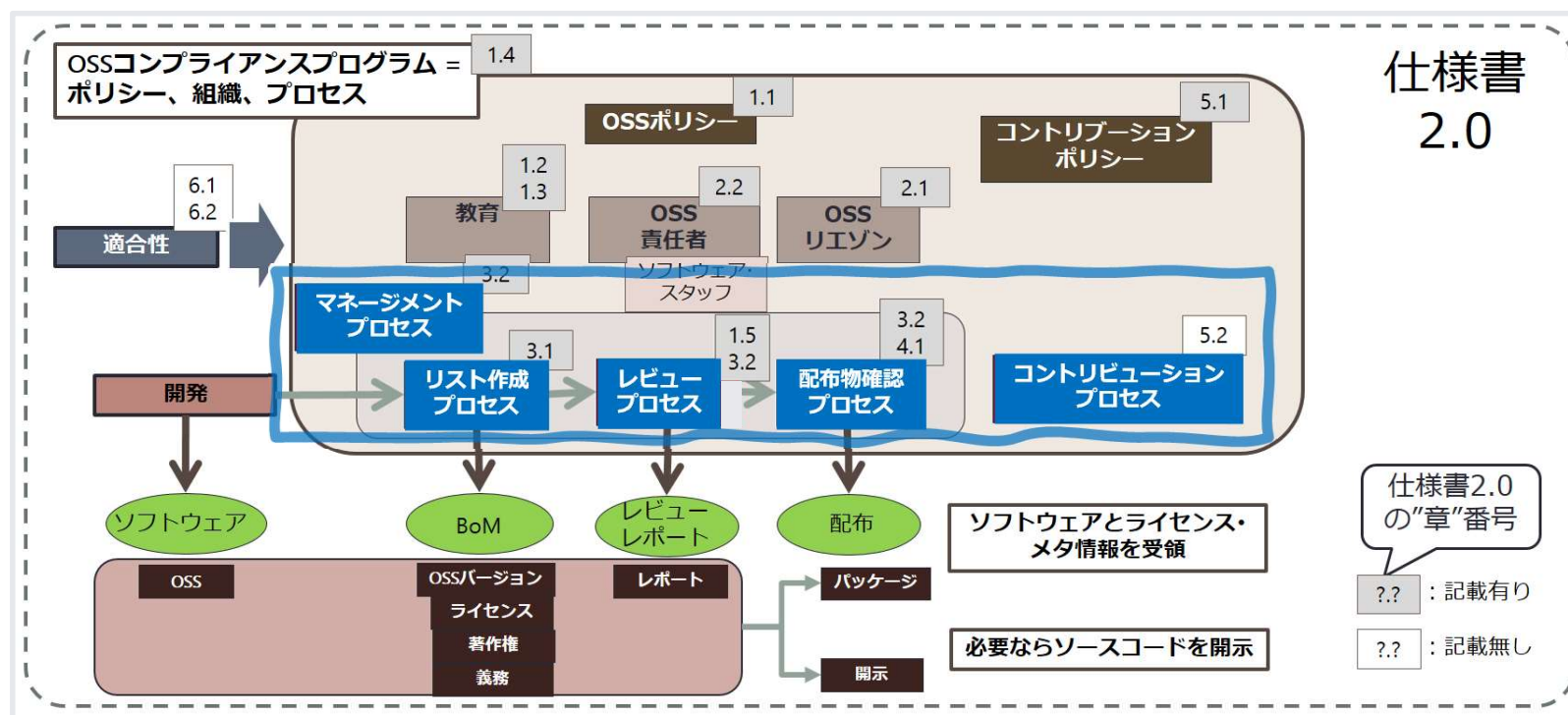
参考 OpenChain Japan Work Group, introduction_2.png, licensed under the CC0-1.0.
 Retrieved from https://github.com/OpenChain-Project/OpenChain-JWG/blob/master/Education_Material/Training/chapters/img/introduction_2.png を一部改変

コンプライアンス体制の例



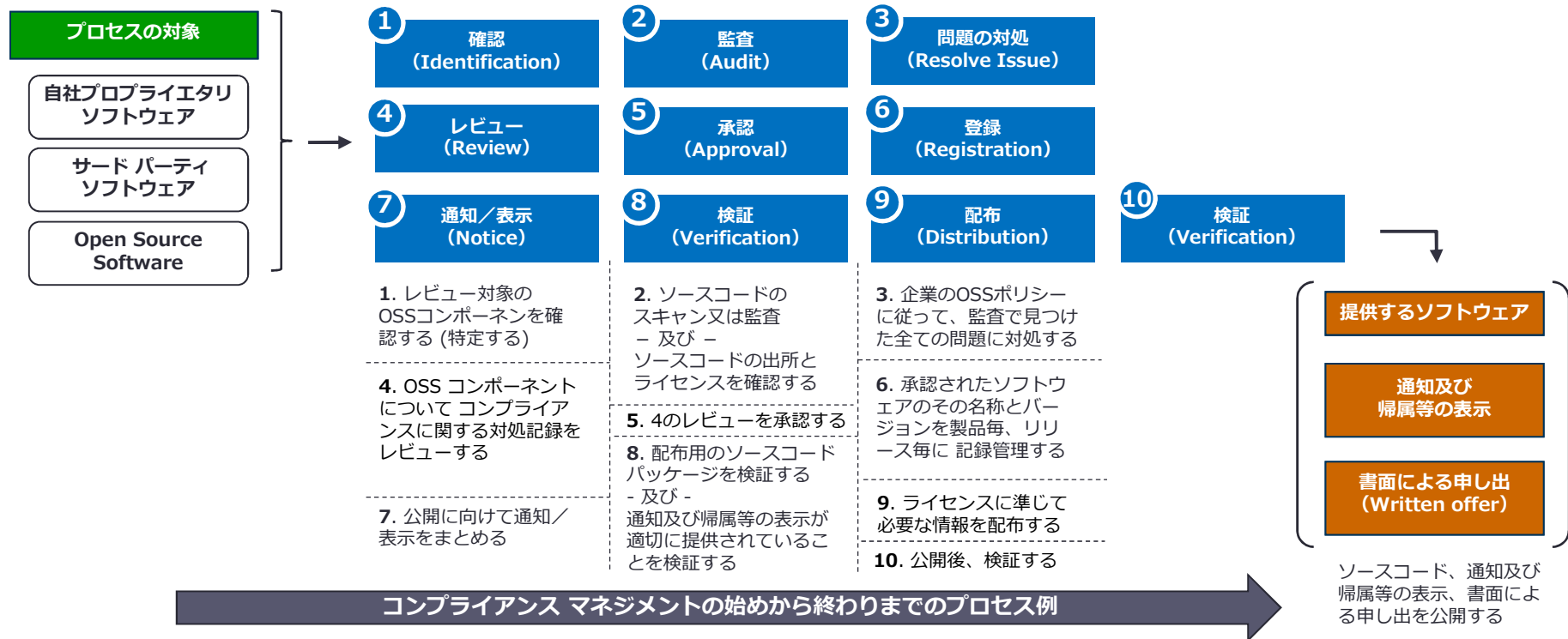
図の出典 OpenChain Japan Work Group, iOSSComplianceOrganization.png, licensed under the CC0-1.0,
 Retrieved from https://github.com/OpenChain-Project/OpenChain-JWG/blob/master/Education_Material/Training/chapters/img/OSSComplianceOrganization.png

OpenChain Specification 2.0 の概観



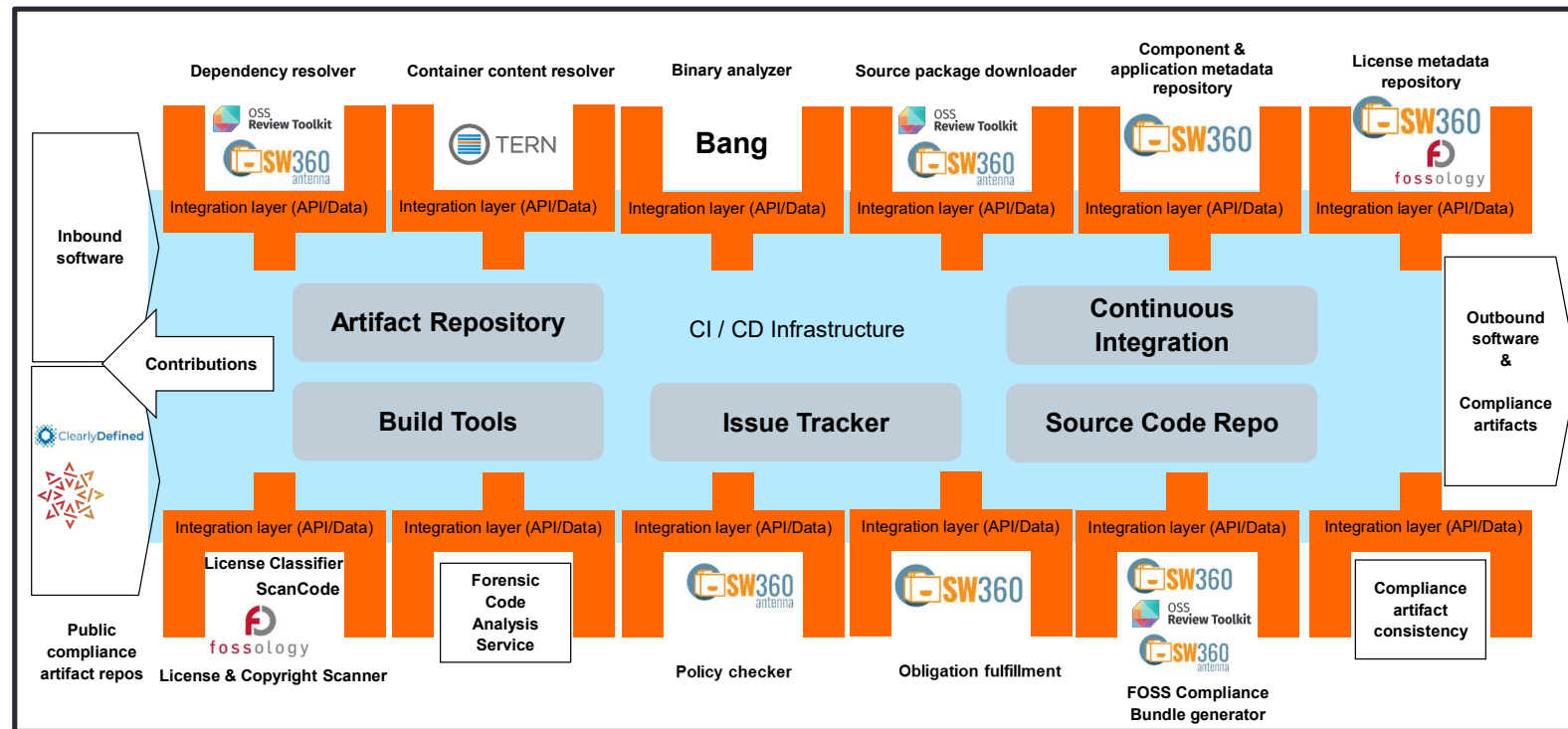
参考 OpenChain Japan Work Group, introduction_2.png, licensed under the CC0-1.0.
 Retrieved from https://github.com/OpenChain-Project/OpenChain-JWG/blob/master/Education_Material/Training/chapters/img/introduction_2.png を一部改変

プロセスの流れの例



参考 OpenChain Japan Work Group, OpenChain カリキュラム (FOSSトレーニング リファレンス スライド OpenChain 仕様書 1.1版対応), licensed under the CC0-1.0.
Retrieved from https://github.com/OpenChain-Project/Reference-Material/blob/master/Training-Slides/Community/jp/1.1/openchain-curriculum-for-1-1_JP.pptx を元に作成

OSS管理とその自動化のためのOSS (Tools)



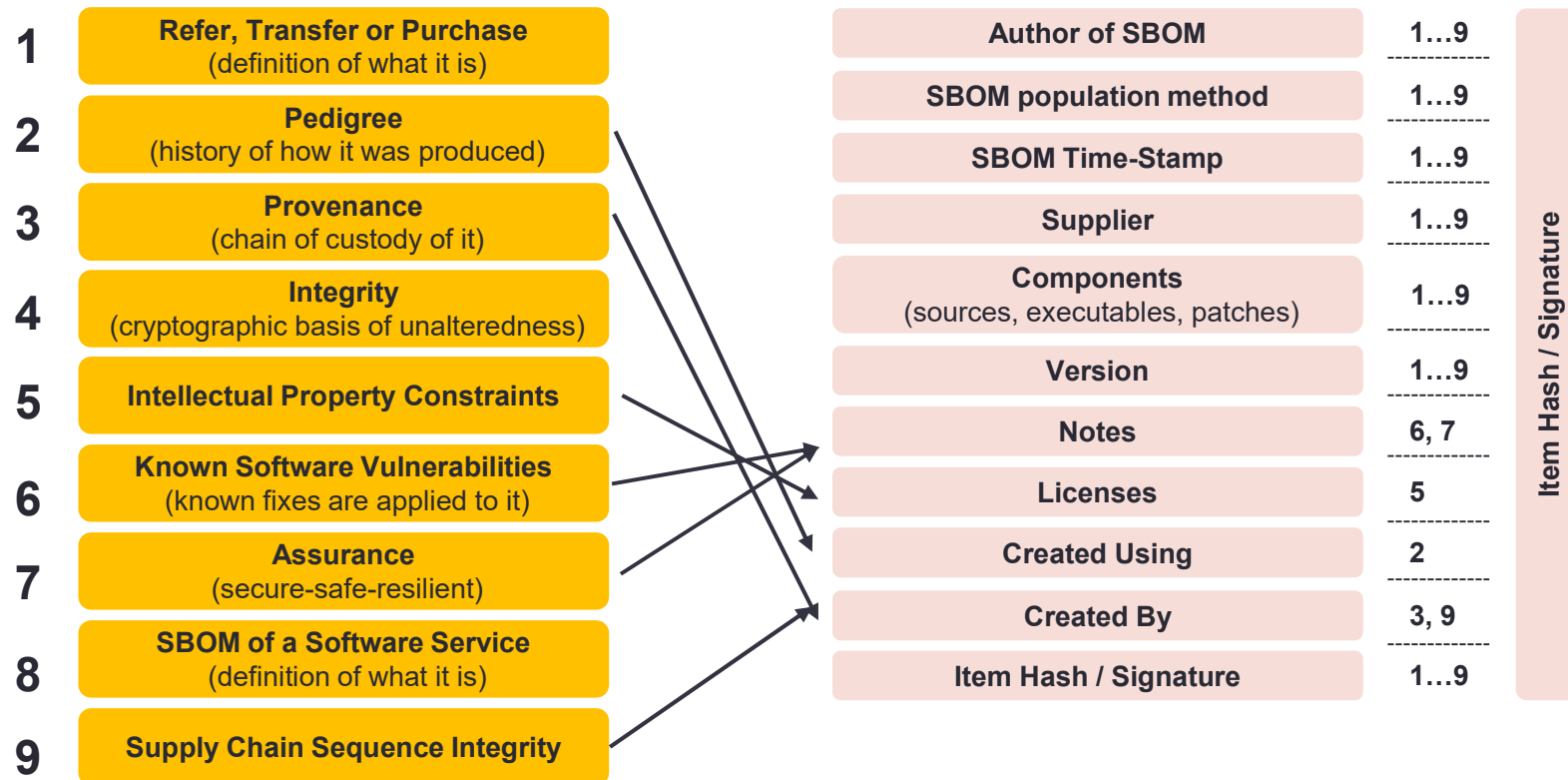
図の出典 Sebastian Schuberth, Bosch: AN UPDATE ON OUR ACTIVITIES IN AUTOMATING OSS COMPLIANCE: A WORKING SHOWCASE, p.7, licensed under the CC0-1.0.
 Presentation in OpenChain Automotive Workshop, October 29, 2019.
 Retrieved from <https://www.slideshare.net/ShaneCoughlan3/bosch-an-update-on-our-activities-in-automating-oss-compliance-a-working-showcase> より、一部改変

OpenChain Japan Work Group / Tooling Sub-Group

Licensed under CC0-1.0

Toshiba Corporation

SBOMのユースシナリオと要素の例 (注: C-SCRMの場合)



参考 Robert A. Martin, Software Bill of Materials (SBOM), pp.16-25. Presentation in SSCA (Software and Supply Chain Assurance) Winter Forum 2020, January 11, 2020.
Retrieved from https://csrc.nist.gov/CSRC/media/Projects/cyber-supply-chain-risk-management/documents/SSCA/2020%20Jan/TuePM2.2_SBOM.pdf より作成

ありがとうございました



Tooling SG : の情報や参加方法

日本語中心でOK

1. Github

- ・ (<https://openchain-project.github.io/OpenChain-JWG/subgroups/tooling/>)

2. メーリングリスト

- ・ (<https://lists.openchainproject.org/g/japan-sg-tooling/>)

3. Slack #tooling-sg

- ・ (<https://openchain-japanwg.slack.com/archives/CGHP86Y4T>)

4. 会合

- ・ (1-2ヶ月に一度の開催)

Tooling SG : 次回会合の案内

日時 : 2020年5月20日(水) 10:00-12:00

場所 : オンライン開催

お題 : 自由

- 発表者を募集します！
- 発表申込手順等、メーリングリストとSlackで案内予定