
OpenChain Japan WG
第6回「組織間のライセンス情報授受」SWGミーティング

日時：2019年2月13日 (水) 15:45-17:30
場所：日立製作所 品川オフィス
参加者：
ソニー：福地さん、小保田さん
トヨタ自動車：遠藤さん、阿部さん
富士通：大内さん
富士通コンピュータテクノロジーズ：安倍さん
パイオニア：當麻さん
パナソニック：加藤さん
オリンパス：小泉さん
デンソーテン：日下部さん
ルネサス：伊藤さん
東芝：野末さん
Linux Foundation：Shaneさん
日立：野村、今田
議事：(主なもの)

(1)SPDXチームとのテレカン情報共有
・手書き(＝手作業で作成)で作成するとしても、SPDXフォーマットに従った方がツールで扱えるなどメリットがある。以下の必須項目は入れて置いた方が良いとSPDXチームから提案を受けた。
- Package SPDX Identifier
- Files Analyzed (手書きなのでfalseと入れておく)

他の必須項目の扱いは質問中。
・SPDX Lightは、SPDXのプロファイルとして取り込んでもらえそうな感触。
プロファイルとして取り込まれれば、SPDXの仕様の一部となるので扱いやすい。
継続して議論し、取り込んでもらえるように活動する。
・SPDX Light はデファクトになりつつあり、その単語で会話が出来るようになって来た。
・次期SPDXの改定で、脆弱性に関する項目追加の提案がありそう。

(2)再低減必要な項目の議論
(a)プログラムの構成によるライセンス情報の範囲
・OSSを利用しているがOSSは含まれないパッケージ(後述)の場合、利用しているOSSの情報は再低減必要な情報として含めない。
契約や、業界別の運用ガイドラインとしてトヨタ自動車さん提案の『要求元からの依頼に関する情報』に追加する。
【議論】
- 脆弱性や、納入時の確認時に利用OSSの情報は欲しい。
- パッケージにOSSが含まれないので、含まれるものと、利用してるものとに分ける必要がある。
- SPDXがパッケージに含まれるモノのライセンス情報を表すものだとすると、利用しているOSSは再低減必要な項目としては適さないのではないか？
- 検証した環境の情報として、OSSのバージョンを書かせている事例はある。
- 2者間契約や、業界としての運用を定める際、要求元が必要な情報があり得る。そちらで検討を進めるのが妥当。

(b)パッケージの単位に関する議論
・差し替え可能な単位をパッケージとし、その単位でライセンス情報を作成する。
【議論】
- 多数のプログラムを一まとめにして納入する場合、一つのSPDXで表そうとすると、巨大なものが出来上がってしまう。
- ライブラリなど、差し替え可能で独立している場合、その単位でライセンス情報を作成すると扱い易い。

(c)手書きサンプルを用いた議論
・Package Download Locationは、OSSの利用者がどこから取得したかを書かないと、OSSの提供者が決められるものでは無いため(forkや、maven等のリポジトリからも公開されることになるため)、利用OSSのライセンス情報を使う側が修正することになる。

・記述方法に制約を付けた方が、書きやすいし、混乱が無くなりそう。
・さまざまなパターンで書いてみると、新たな課題が見つかることもある。
・Excel形式のSPDX情報を変換するツールもありそう。活用できるツールの調査も
　行えると良い(★今後のアクション)。

(3)企業間ライセンス情報授受に関するガイドラインの作成
・本SWGのアウトプットとして、ガイドラインの作成を計画している。
・現状検討中の目次をベースに、骨組みを作成するので、SWGメンバでレビュー、
　執筆の分担をさせて欲しい(★今後のアクション)。
・目次案はGithubに英語版も作って登録してSPDXチームに意見を貰うようにする。
・ガイドライン作成時など、実際に使われているSPDXの例があると良い。
　(★今後のアクション)

(4)今後のアクション
・2/29 三菱電機さんで実施のJapanWGには、活動状況を報告する。
　事前に資料を展開するので、確認をお願いします。　担当:日立
・ガイドラインの目次案(日本語,英語)をGithubに登録　担当:日立
・ガイドランの骨格を作成してレビュー展開　担当:日立
・SPDXの実例収集と共有　担当:デンソーテン

(5)次回
・メールにて議論し、必要に応じてFace to Faceを開催する。

以上