"Open Source Compliance Recommended Practices For Compliance Professionals"

オープンソース コンプライアンス

コンプライアンス プロフェッショナル向け推奨プラクティス

- Compliance is verified on a product-by-product basis: If an open source component is approved for use in one product, it does not necessarily mean it is pre-approved for use in other products.

◆ **プロダクト毎にコンプライアンスが確認されている**：オープンソースのコンポーネントがプロダクトの一つで使用されることが承認されていても、他のプロダクトで事前承認されているという意味にはならない

- Scan all source code, early and often. It allows you to discover compliance problems as they occur, provide solutions within acceptable delays, and perform incremental compliance very efficiently.

◆ **すべてのソースコードを早期に、かつ頻繁にスキャンしている**。それによりコンプライアンス問題が発生した時に発見でき、許容可能な遅れの範囲での解決策提供を可能とし、そして成長型の（Incremental）コンプライアンスを行うことができる

- Inspect and resolve each file or snippet flagged by the scanning tool.

◆ スキャン ツールでフラグのついた**ファイルやスニペット[1]一つ一つに対しインスペクションを行い**、解決している

- When in doubt with the scan results discuss with engineering.

◆スキャン結果に疑問がある際に**エンジアリングチームとの議論**を実施している

- Identify all the components and snippets included in the product, their origin and licenses.

◆ プロダクトに含まれる**コンポーネントとスニペットと、それらの出所(Origin)やライセンスがすべて特定**されている

- Scan newer used versions of previously approved packages.

◆ 以前承認されたパッケージについて、新しい方の使用バージョンをスキャンしている

- If the scanning tool identifies GPL-licensed source code (for instance) integrated in a proprietary component, report to Engineering and request correction. Re-scan the code after Engineering has resolved the issue to get a solid confirmation that GPL code has been replaced.

◆ スキャン ツールが **GPL ライセンスのソースコードを特定し**、（たとえば）それがプロプライエタリ コンポーネントに統合されていることが分かった場合、エンジニアリング チームに報告し、訂正を要請している。エンジニアリング チームが問題を解決し、GPL コードがリプレースされたことをしっかり確認するために**再スキャンを実施**している

[1] （Weblio 辞書「スニペット」から）「スニペットとは、一般的には「切れ端」「断片」という意味の英語である。IT 用語としては、プログラミング言語の中で簡単に切り貼りして再利用できる部分のこと、（中略）プログラムを作成する際には、しばしば、頻繁に利用する同じ記述の繰り返しや、微妙な変更を加えるだけで使うことができそうなパターンに遭遇する。そのようなパターンをスニペットとして登録しておくと、一塊のコードを呼び出して貼り付けることで簡単に記述できるようになる。」

Ibrahim Haddad, Ph.D. Twitter:@IbrahimAtLinux

- In preparation of legal review, provide Legal with all licensing information discovered in the component. For open source components, that includes COPYING, README, or LICENSE files.

◆ リーガル レビューの準備において、コンポーネントで発見された**すべてのライセンス情報をリーガル チームに提供**している。オープンソースのコンポーネントについては、COPYING、README、LISENCE といったファイルがこれに含まれる

- If there are conflicts or compliance is not possible:

  a. Remove / Replace: Can you live without this code? Is there an alternative project with same function under a different license?

  b. Re-engineer: Can you create a work around?

  c. Version tracking: Is there a newer (or older) version of this code under a different license?

  d. Re-license: Can you contact the author(s) and ask for a different license?

◆ コンフリクトが発生している、もしくはコンプライアンスができない場合には：

  a. **削除(Remove)、置換(Replace)する**：そのコードなしで済ませることができるか？異なるライセンスで同じ機能をもつプロジェクトを選択できるか？

  b. **再エンジニアリング(Re-engineer)する**：次善策（Work around）を作り出せるか？

  c. **バージョン トラッキングする**：新しい（もしくは古い）バージョンで異なるライセンスのものがあるか？

  d. **再ライセンスする**：著作者（たち）にコンタクトし、異なるライセンスの設定を依頼することができるか？

- Be clear in the language of the written offer

◆ 書面による申し出(Written Offer)の**言葉づかい（Language）が明解**になっている