OpenChain 規範書

版本 2.1

本規範在功能上等同於：

- OpenChain 規範 2.0
- ISO/IEC PRF 5230

了解更多： www.openchainproject.org

內容

簡介

本份文件定義了開源授權合規方案的主要要件以確保其品質。目的是為了建立一個信任基準，以提供組織之間在交換由開源軟體組成的軟體解決方案。規範一致性可確保為開發每個軟體解決方案所需的合規程序（即法律聲明，原始碼等）。相較於「如何」及「何時」的考量，本規範書聚焦於合規方案「什麼」及「為什麼」的特性。如此在實際的操作上，能確保不同的組織在推動政策及進程上增加靈活度，適切選擇符合他們的規模，目標以及範圍。舉例來說，OpenChain 一致性方案可以涵蓋單個產品線或整個組織。

本簡介提供相關訊息給所有的潛在用戶。 第 2 條定義了本文件中使用的關鍵術語。 第 3 條定義了程序一致性必須滿足的要件。此要件必須包含一個或一個以上的審核程序 (即紀錄)所組成。審核程序不需要公開，雖然組織可能會根據保密協議（NDA）選擇將其提供給他人。

本文件是一個開放的倡議，收到了來自 200 多個貢獻者的反饋。 可以通過查看規範郵件列表和常見問題（FAQ）來了解其歷史沿革。

信息技術— OpenChain 規範

1 範圍

本文件定義了開源合規授權方案的主要要件以確保其品質，並建構一套信任標準以提供組織之間在交換由開源軟體組成的軟體解決方案。

2 術語和定義

就本文件而言，適用以下術語和定義。

2.1
合規工件
代表合規程序輸出並隨附提供的軟體工件集成

注意：集成可能包括（但不限於）以下一項或多項：著作權聲明，原始碼，構建和編程，授權條款副本，版權聲明，修改註記，書面報價，開源組件資料清單 和 SPDX 文件。

2.2
確認條款
開源軟體授權是通過一組開源軟體許可認證所遵循的制度。

2.3
OpenChain 一致性
滿足本規範書所有要件的方案。

2.4
開源軟體
軟體程式依據一個或多個授權條款，該條款必須符合開源倡議組織（Open Source Initiative）發布的開源定義（Open Source Definition）（請參閱 opensource.org/osd）或自由軟體基金會（Free Software Foundation）所發布的自由軟體定義（Free Software Definition）（請參見 gnu.org/philosophy/free-sw.html）或類似條款。

2.5
執行程序
用來管理組織內開源授權合規行為的一套政策，流程和人員。

2.6
計劃參與者
對於提供軟體有貢獻或負責準備的任何組織僱員或承包商，進行範圍界定。

注意：根據組織的不同，可能包括（但不限於）軟體開發人員，發布工程師，質量工程師，產品行銷和產品管理。

2.7
SPDX

由 Linux 基金會 SPDX（軟體包數據交換）工作小組制定的標準格式，其目的是為了規範交換給定軟體包的資料清單，包括相關的授權和版權信息，請參閱 www.spdx.org。

2.8
提供的軟體
一個組織交付給第三方的軟體（例如，其他組織或個人）。

2.9
驗證資料
符合規範給定要件的證明資料。

ISO 和 IEC 在以下網址用於維護標準化的術語數據庫：

— ISO Online 瀏覽平台：取得資料 https://www.iso.org/obp

— IEC Electropedia：取得資料 http://www.electropedia.org/

3 要件

3.1 方案基礎

3.1.1政策

具備一份成文且經過內部溝通的開源政策計畫書，此計畫書用於管理交付軟體發布時的開源合規授權。

驗證資料：

- 3.1.1.1 具備一份開源政策計畫書。
- 3.1.1.2 具備一份流程文件，可使所有的軟體參與者了解開源政策計畫的存在（例如，通過培訓，內部 Wiki 或其他實用的交流方法）。

理由說明：

為了確保開源政策計畫書的擬定、紀錄，並使軟體工作人員意識到開源策略的存在。 儘管此處未提出有關什麼內容應包括在計畫書裡，然而其他章節可能會有所要求。

3.1.2權限

組織建議

- 確認和方案執行以及效益之相關角色，以及其相對應的職責;
- 確定履行每個職責的計劃參與者都具備必要的能力;
- 確保計劃參與者透過適當的教育，培訓和/或在經驗的基礎上能夠勝任職務;
- 如有需要，採取行動以獲得必要的能力; 以及
- 保留合適文件資訊以作為證明這些能力的證據。

驗證資料：

- 3.1.2.1 具備一份說明文件，敘述方案中不同參與者的角色以及其相對應的職責。
- 3.1.2.2 具備一份確認文件來敘述每個角色的能力。
- 3.1.2.3 具備一份證明文件評估每個計劃參與者的能力。

理由說明：

確保計劃參與者已經擁有足夠的能力來履行其各自的角色和職責。

3.1.3意識

組織應確保計劃參與者了解：

- 開源政策；
- 相關的開源目標；
- 他們對於方案效益的貢獻；以及
- 不遵守計劃要求的後果。

驗證資料：

- 3.1.3.1 對計劃參與者進行意識評估的確認文件，其中應包括計劃目標，在計劃中的貢獻以及是否意識到未能遵守計劃所影響的含義。

理由說明：

為確保計劃參與者對他們在計劃中的各自角色和職責有充分的了解。

3.1.4計劃範圍

不同的方案可能受不同級別範圍所管轄。 例如，一個方案可以管理單一產品線，整個部門或整個組織。每一個方案須聲明其方案之指定範圍。

驗證資料：

- 3.1.4.1 以書面陳述，明確定義出本方案的範圍和限制。

理由說明：

為了彈性化構建最適合組織需求範圍而設計。 有些組織可以選擇維護特定產品線的方案，而其他組織則可以實行一個方案來管理整個組織架構的軟體。

3.1.5授權義務

應具備一個流程用於審查已確定的授權，以確保每個授權條款授與的權利、義務及其限制。

驗證資料：

- 3.1.5.1 以書面的程序，審查和記錄每個已確定的授權授予的權利、義務和限制。

理由說明：

為確保針對在組織可能遇到的各種案例（如第 3.3.2 中所定義），對於每個已進行中的授權案的審查和確保授權義務的過程。

3.2 定義和支持相關任務

3.2.1途徑

維護一個有效回應外部開源查詢的管道 。 公開一個第三方可以進行開源合規性查詢的方法。

驗證資料：

- 3.2.1.1 具備公開可見的方法，允許任何第三方進行開源授權合規性查詢（例如，透過電子郵件或 Linux Foundation 開源合規平台）。
- 3.2.1.2 具備內部流程控管的程序，用於回應第三方開源授權合規性查詢。

理由說明：

確保組織具備一個便捷合理的方法，能夠聯繫以及有效回應來自第三方開源授權合規性查詢。

3.2.2資源有效化

資源計劃的任務和確認項目：

- 分配責任以確保任務成功執行。
- 任務方案具備充份資源:
  - 已經分配了執行任務的時間； 和
  - 已經配置充足的資金。
- 具備一個用於審查和更新政策及支持任務的流程；
- 需要指導的人可以獲取有關遵守開源合規的法律專業知識； 和
- 具備解決開源合規爭議的流程。

驗證資料：

- 3.2.2.1 標識計劃方案中的人員，團體或職責名稱的文件。
- 3.2.2.2 確定計劃方案已經配備了適當的人員，並提供充足的資金。
- 3.2.2.3 確認擁有內部或外部法律專業知識以解決開源授權合規事項。
- 3.2.2.4 具備一份流程文件，該程序明訂了開源合規性的內部責任。
- 3.2.2.5 具備一份流程文件，來審查和處理不合規案件。

理由說明：

確保：i）有效支持計劃方案，採責任制並提供資源； ii）定期更新政策及支持流程，以適應開源合規的變化並達到最佳化的進展。

3.3 開源內容審查和批准

3.3.1物料清單

具備一個流程用來建立以及管理物料清單，該物料清單包含交付軟體中每一個開源組件 (以及確認授權條款)。

驗證資料：

- 3.3.1.1 具備一份流程文件，用於確認，追蹤，考核，批准和建檔有關開源組件交付軟體的信息。
- 3.3.1.2 每個交付軟體皆須具備開源組件紀錄，以證明該流程被正確的執行。

理由說明：

為了確保具備一個流程能夠建立以及管理交付軟體中的開源組件物料清單。該清單用來支持有系統的審查和批准每個組件的授權條款，以解析適用於交付軟體中所遵循的義務和限制。

3.3.2授權條款合規性

此方案必須能夠管理軟體工作人員在處理交付軟體上，時常會碰到的開源授權條款使用案例，其中可能包括下列使用案例（注意本列表並未詳盡，亦可能不適用於所有用例）:

- 以二進位執行檔形式散布；
- 以原始碼形式散布；
- 與其他開放原始碼整合而可能觸發額外的許可義務性要求；
- 包含修改後的開放原始碼；
- 包含開放原始碼或其他軟體，其中與交付軟體裡其他互動元件不相容的授權條款；及／或
- 包含具有署名要求的開放原始碼。

驗證資料：

- 3.3.2.1 具備一份流程文件，來審查和處理在交付軟體的開源組件中常見的開放原始碼授權使用案例。

理由說明：

為確保該程序具有足夠的相容性，並遵循支持該活動以處理組織中常見的開源授權使用案例。

3.4 合規工件的創建和交付

3.4.1合規工件

具備一個流程，為交付軟體創建一組合規工件。

驗證資料：

- 3.4.1.1 具備一份流程文件，用於描述確保遵從隨付軟體進行準備和發布合規工件時，該過程必須滿足授權條款之要求。
- 3.4.1.2 歸檔的過程，具備一份流程文件來描述交付軟體中合規工件副本的歸檔程序 - 此檔案從最後遞交交付軟體後至少需保存一段合理的時間[1]; 或者根據授權條款中的要求(以較長者為準)。此外，須留存相關紀錄，以證明已確實遵循該程序。

理由說明：

為確保已確定的授權要求，在商業層面上盡一切合理的努力準備交附軟體的合規工件。

3.5 了解開源社群參與

3.5.1貢獻

如果一個組織考慮對開源專案做出貢獻，則

- 應當制定書面政策來管理對開源專案的貢獻；

[1] 取決於網域司法管轄權或是透過客戶合約內容

- 該政策應在內部傳達；以及
- 此政策必須具備一個流程來執行

驗證資料：

如果一個組織允許對開源項目做出貢獻，則應俱備以下條件：

- 3.5.1.1 開源貢獻政策書的制定；
- 3.5.1.2 規範開源程序的書面資料；和
- 3.5.1.3 在擬定計畫書的過程，應讓使所有程序參與者都知道開源貢獻政策的存在（例如，通過培訓，內部 Wiki 或其他實用的交流方法）。

理由說明：

當一個組織允許開源貢獻時，我們希望該組織已充分考慮來製定及實施貢獻政策。 開源貢獻政策可以是整體開源策略的一部分，也可以是一個獨立的策略。

3.6 遵守規範要件

3.6.1符合標準

為了使程序符合 OpenChain 的規範，組織應確認該程序符合了本文檔中提出的要求。

驗證資料：

- 3.6.1.1 具備一份文件以確認§3.1.4 中提到的方案已滿足本規範書的所有要求。

理由說明：

為確定一個組織是否如其宣稱擁有符合 OpenChain 程序的方案，則該方案必須達到本規範書記載的所有要件。若僅是達到這些要件的一部份則是不夠的。

3.6.2持續期間

符合此版本規範的 OpenChain 程序，應自獲得合規性驗證之日起至少持續 18 個月。合規性驗證註冊過程可以在 OpenChain 項目的網站上找到。

驗證資料：

- 3.6.2.1 在獲得合規性驗證的過去 18 個月內，需具備一份已滿足本規範書所有要件的計畫案。

理由說明：

如果一個組織希望長時間宣稱其方案是持續遵守本規範的要求，則須與本規範的最新版本保持同步。此要求確保該方案的支持流程與管理不會逐步喪失。

附錄 A
(有用信息)

本規範的語言翻譯

為了促進全球採用，非常歡迎將規範書翻譯成多種語言。由於 OpenChain 採開源專案方式運作，翻譯亦由那些願意貢獻他們時間與專業的人士所推動，i)根據 CC-BY-4.0 授權及　ii)本專案的翻譯政策來進行。本政策的細節及現有翻譯可在 OpenChain 專案規範書網頁上找到。