OPENCHAIN

OpenChain Conformance Specification (한국어)

Version 1.0

Contents

Disclaimer

이 문서는 OpenChain Project 의 공식 번역본입니다. 원본인 영문 문서에서 번역되었습니다.
번역본과 영문판이 혼동되는 경우, 영문 문서가 우선합니다.

This is an official translation from the OpenChain Project. It has been translated from the original English text. In the event there is confusion between a translation and the English version, The English text shall take precedence.

Copyright and License

소개

OpenChain Initiative 는 2013 년, 한 Software 공급망 (Supply Chain) Open Source 전문가 그룹이 다음과 같은 두 가지 새로운 패턴을 관찰하면서 시작되었다. : 1) 성숙한 Open Source Compliance Program 이 있는 조직 간에는 상당한 Process 유사성이 존재함; 2) 이러한 Program 을 갖추지 못한 상태로 Software 를 교환하는 조직도 여전히 많이 존재하고 있음. 여기에서 두 번째 패턴으로 인해 Software 교환 시 동봉해야 하는 Compliance 산출물의 일관성 및 품질에 대한 신뢰를 떨어지게 되었다. 결과적으로 Software 공급망 내 각 계층에서의 Downstream 조직은 Upstream 조직에서 이미 수행한 Compliance 작업을 다시 수행하는 일이 자주 발생하게 되었다.

이에 한 Study Group 이 다음과 같은 Standard Program Specification 의 제작을 고려하기 위해 구성되었다.: i) 업계에서 공유되는 Open Source Compliance 정보의 품질과 일관성 향상; ii) Compliance 재작업으로 인해 발생하는 높은 Open Source 관련 거래 비용의 절감. 이 Study Group 은 Work Group 으로 발전하였으며, 2016 년 4 월에는 Linux Foundation Collaborative Project 로 정식 조직되었다.

OpenChain Initiative 의 Vision 과 Mission 은 다음과 같다:

- **Vision**: Free/Open Source Software(FOSS)를 신뢰할 수 있고 일관된 Compliance 정보와 함께 제공하는 Software 공급망
- **Mission**: Software 공급망 참가자를 위해, Free/Open Source Software(FOSS)의 효과적인 관리를 위한 요구사항을 수립하여 요구사항 및 부수적인 관련 사항을 Software 공급망, Open Source Community 및 학계 대표자가 공동으로, 또한 공개적으로 개발할 수 있도록 한다.

Vision 과 Mission 에 따라 이 Specification 일련의 요구사항을 정의하고, 이 요구사항이 충족하는 Open Source Program 이라면 충분한 수준의 품질, 일관성 및 완전성을 달성했을 가능성을 높일 것이다. 다만, Specification 의 모든 요구사항을 만족하는 Program 이라도 완전한 Compliance 가 보장되는 것은 아니다. 이 요구사항은 Program 이 OpenChain 을 따르는 것으로 간주하기 위해 충족해야 하는 기본 수준 (최소) 요구 사항 집합을 나타낸다. 이 Specification 은 "How"와 "When"에 대한 고려가 아닌 Compliance Program 의 "What"과 "Why"에 대해 초점을 맞추고 있다. 이는 서로 다른 조직이 각자의 목적에 가장 잘 부합하도록 정책과 프로세스를 조정할 수 있게 하는 실질적인

유연성을 보장한다.

Section 2 에서는 Specification 전체에 걸쳐서 사용되는 주요 용어의 정의를 소개한다. Section 3 에서는 각 Specification 요구사항에 대해 하나 혹은 그 이상의 Verification Artifact(확인 산출물) 목록을 제시한다. 이들은 주어진 요구사항이 만족한 것으로 간주하기 위해 필요한 증거이다. 어떤 Program 이 모든 요구사항을 충족한다면, 그 Program 은 이 Specification version 1.0 에 따라 OpenChain Conforming(OpenChain 을 따르는 것)으로 간주할 수 있다.

정의

Distributed Compliance Artifacts(배포된 Compliance 산출물) - 식별된 License 가 요구하는 일련의 산출물 세트 (Supplied Software 와 함께 제공됨). 여기에는 다음 사항이 포함된다 (이에 국한되지 않음). : 저작권 고지, License 사본, 수정 내용 고지, 저작자 고지, Source Code, Written Offer 등

FOSS (Free and Open Source Software) - Open Source Initiative (OpenSource.org)에서 발표한 Open Source 정의 혹은 Free Software Foundation 에서 발표한 Free Software 정의를 충족하는 License, 혹은 유사한 License 가 하나 이상 적용된 Software.

FOSS Liaison (연락담당자) - 외부 FOSS 문의를 받도록 지정된 사람.

Identified (식별된) Licenses - 해당 License 를 식별하기 위한 적절한 방법을 수행한 결과를 통해 식별된 FOSS License 세트.

OpenChain Conforming (OpenChain 을 따르는것) – 이 Specification 의 모든 요구사항을 만족하게 하는 Program.

Software Staff - Supplied Software 를 준비하기 위해 정의, 기여하거나 책임을 지는 모든 직원 또는 계약자. 조직에 따라 Software 개발자, Release Engineer, 품질 Engineer, 제품 마케팅 및 제품 관리자가 포함될 수 있지만, 이에 국한되지 않는다.

SPDX (Software Package Data Exchange) – Software Package 에 대한 License 및 저작권 정보를 교환하기 위해 SPDX Working Group 이 만든 표준 형식이다. SPDX Specification 에 대한 설명은 www.spdx.org 에서 확인할 수 있다.

Supplied Software – 한 조직에서 제 3 자(예: 다른 조직 혹은 개인)에게 제공하는 Software.

Verification Artifacts - (확인 산출물) - 주어진 요구사항을 만족한 것으로 판단하기 위해 존재해야 하는 증빙.

요구사항

G1: 당신의 FOSS 책임을 이해하라

1.1 문서로 만들어진 FOSS 정책이 존재하고, 이를 통해 Supplied Software 배포 시에 필요한 FOSS License Compliance 를 관리한다. 이 정책은 최소 내부에서 접근할 수 있는 공간에 존재한다.

Verification Artifact(s) (결과물 확인):

- 1.1.1 문서로 만들어진 FOSS 정책이 존재한다.
- 1.1.2 모든 Software Staff 가 FOSS 정책의 존재를 인식할 수 있도록 문서로 만들어진 절차(예: Traning, 내부 wiki 혹은 기타 실잘직인 의사소통 방법)가 존재한다.

Rationale (방법):

FOSS 정책을 생성 및 기록하고 이를 Software Staff 가 인식하게 할 수 있는 조치가 취해졌는지 확인하라. 여기서는 정책 내에 무엇이 포함되어야만 하는지에 대해서는 요구하고 있지 않지만, 다른 섹션에서는 다른 요구사항이 있을 것이다.

1.2 모든 Software Staff 대상으로 하는 다음과 같은 필수 FOSS Training 이 존재한다:

- **Training 은 최소한 다음 주제를 다룬다:**
  - **FOSS 정책 및 사본을 찾을 수 있는 곳;**
  - **FOSS 및 FOSS License 에 관한 IP 법의 기본;**
  - **FOSS Licensing 개념 (Permissive 및 Copyleft 개념 포함);**
  - **FOSS Project Licensing 모델;**
  - **세부적인 FOSS Compliance 및 전반적인 FOSS 정책에 관한 Software Staff 의 역할 및 책임;**
  - **Supplied Software 에 포함된 FOSS Component 의 식별, 기록 및 추적을 위한 Process.**
- **Software Staff 는 지난 24 개월(현재로 간주함)내 FOSS Training 을 완료해야 한다. 때, Test 를 통해 Software Staff 가 Training 요구사항을 만족하는지 확인할 수도 있다.**

Verification Artifact(s) (결과물 확인):

- 1.2.1 위의 주제를 다루는 FOSS 과정 자료(예: Slide 자료, Online 과정 혹은 이외 Training 자료)가 존재한다.
- 1.2.2 모든 Software Staff 가 과정을 완료하였는지 추적하는 방법.
- 1.2.3 적어도 Software Staff 의 85%가 현재 (위에서 정의한) 완료한 상태.

Rationale (방법):

Software Staff 가 최근 FOSS Training 에 참석했는지, FOSS Training 이 핵심 FOSS 주제를

다루는지를 확인한다. 이 의도는 핵심 기본 수준의 주제를 다루는 것이지만, 일반적인 Training Program 은 여기서 요구하는 것보다 더 포괄적일 수도 있다.

G2: Compliance 달성을 위한 책임을 할당하라

2.1 FOSS Liaison (연락담당자)의 기능을 확인한다.

- **FOSS 관련 외부 문의 대응을 책임질 인원을 지정한다;**
- **FOSS Liaison (연락담당자)는 타당한 FOSS Compliance 문의에 대응하기 위해 상업적으로 합당한 노력을 해야 한다. 그리고,**
- **전자 통신을 통해 FOSS Liaison (연락담당자)에게 연락할 방법이 공개되어있는지 확인한다.**

Verification Artifact(s) (결과물 확인):

⌋ 2.1.1 FOSS Liaison (연락담당자) 기능이 공개적으로 확인된다. (예: Email 주소 혹은 Linux Foundation 의 Open Compliance Directory 를 통해).

⌋ 2.1.2 FOSS Compliance 문의에 대응하기 위한 책임을 할당하는 문서로 만들어진 절차가 존재한다.

Rationale (방법):

제 3 자가 FOSS Compliance 문의와 관련하여 조직에 연락할 수 있는 합리적인 방법이 있는지 확인한다.

2.2 내부 FOSS Compliance 담당을 확인한다.

- **내부 FOSS Compliance 를 관리할 인원을 지정한다. FOSS Compliance 담당과 FOSS Liaison (연락담당자)는 동일 인원이 될 수 있다.**
- **FOSS Compliance 관리 활동에는 충분한 자원이 있다.**
- **담당자로서 임무를 수행할 시간이 할당된다.**
- **상업적으로 합당한 예산이 배정된다.**
- **FOSS 정책 및 Process 를 개발하고 유지할 책임을 할당한다.**
- **FOSS Compliance 담당은 FOSS Compliance 에 대한 (내외부) 법률 전문 지식에 접근할 수 있다.**
- **FOSS Compliance 이슈의 해결을 위한 Escalation 이 가능하다.**

Verification Artifact(s) (결과물 확인):

⌋ 2.2.1 지정된 FOSS Compliance 담당자, 조직 혹은 직무 이름.

⌋ 2.2.2 FOSS Compliance 담당이 사용할 수 있는 법률 전문 지식의 제공처를 확인한다.

⌋ 2.2.3 FOSS Compliance 에 대한 책임을 할당할 수 있는 문서로 만들어진 절차가 존재한다.

⌋ 2.2.4 이슈 해결을 위한 Escalation 경로를 확인하는 문서로 만들어진 절차가 존재한다.

Rationale (방법):

FOSS 책임이 효과적으로 할당되었는지 확인한다.

G3: FOSS Content 를 Review 하고 승인하라

3.1 Supplied Software 가 포함하는 모든 FOSS Component(및 각각 식별된 License)를 확인, 추적 및 보관하는 Process 가 존재한다.

Verification Artifact(s) (결과물 확인):

⌋ 3.1.1 Supplied Software 가 포함하는 FOSS Component 및 식별된 License 목록을 확인, 추적, 보관하는 문서로 만들어진 절차가 존재한다.

Rationale (방법):

Supplied Software 를 구성하기 위해 사용된 모든 FOSS Component 를 확인 및 나열하기 위한 Process 가 존재하는지 확인한다. 이는 Supplied Software 에 적용되는 각 Component 의 배포 의무 및 제한 사항을 이해하기 위해 License 조항을 체계적 Review 할 수 있도록 존재해야 한다. 또한, 이 기록된 목록은 Process 가 수행되었다는 증빙으로 사용된다.

3.2 3.2 FOSS Program 은 Supplied Software 에 대해 Software Staff 가 접하게 되는 일반적인 FOSS Use Case 를 처리할 수 있어야 하고, 여기에는 다음과 같은 Use Case 가 포함될 수 있다. - (아래 리스트가 모든 경우를 포함하지는 않으며 또한, 조직에 따라 아래의 모든 사항이 적용되는 것은 아님) Supplied Software 의 일부가:

- **Binary Form 으로 배포되는 경우**
- **Source Form 으로 배포되는 경우**
- **다른 FOSS 와 통합되어 Copyleft 의무 사항을 유발하는 경우**
- **수정한 FOSS 를 포함하는 경우**
- **FOSS 혹은 Supplied Sofware 내 다른 Component 와 상호 작용하면서 호환되지 않는 License 하에 있는 다른 Software 를 포함하는 경우**
- **저작자 표시 요구사항이 있는 FOSS 를 포함하는 경우**

Verification Artifact(s) (결과물 확인):

⌋ 3.2.1 Supplied Software 에 대해 Software Staff 가 접할 수 있는 일반적인 FOSS Use Case 를 처리할 수 있는 Process 가 구현되었다.

Rationale (방법):

FOSS Program 이 해당 조직의 Business 업무를 고려했을 때, 전형적인 User Case 를 다루기에 충분히 견고하도록 만든다.

G4: FOSS Content 문서 및 Artifact(결과물)을 제공하라

4.1 해당하는 식별된 License 에서 요구하는 대로 Supplied Software 와 함께 제공하기 위한 다음의 Distributed Compliance Artifact 을 준비한다. 여기에는 다음 내용이 포함될 수 있지만, 이에 국한되지는 않는다:

- **저작권 고지(Copyright Notices)**
- **식별된 License 의 사본**
- **수정 고지**
- **저작자 표시 (Attribution Notices)**
- **Prominent Notice**
- **Source Code**
- **요구되는 Build 방법 및 Script**
- **Written Offer**

Verification Artifact(s) (결과물 확인):

⌋ 4.1.1 식별된 License 에서 요구하는대로 Supplied Software 와 함께 Distributed Compliance Artifact 가 배포되도록 보장하는 Process 를 설명하는 문서로 만들어진 절차가 존재한다.

⌋ 4.1.2 Distributed Compliance Artifact 의 사본이 보관되고 쉽게 검색할 수 있다 (예: Legal Notice, Source Code, SPDX 문서). 보관된 자료는 적어도 Supplied Software 가 제공되는 한 혹은 식별된 License 에서 요구하는 기한 동안 존재하여지도록 한다 (둘 중 더 긴 것을 따름).

Rationale (방법):

Supplied Software 에 적용되는 식별된 License 에서 요구하는 대로 완전한 Compliance 산출물 집합이 Supplied Software 와 함께 제공되는지 확인한다.

G5: FOSS Community 로의 참여를 이해하라

5.1 조직 대신 직원들이 공개적으로 접근 가능한 FOSS Project 에 Contribution 하는 것을 관리하기 위한 문서로 만들어진 정책이 존재한다. 이는 최소 내부에서 접근할 수 있는 공간에 존재만 한다.

Verification Artifact(s) (결과물 확인):

- 5.1.1 문서로 만들어진 FOSS Contribution 정책이 존재한다;
- 5.1.2 모든 Software Staff 가 FOSS Contribution 정책의 존재를 알도록 하는 문서로 만들어진 절차(예: 교육, 내부 wiki, 혹은 다른 실제적인 의사소통 방법을 통해)가 존재한다.

Rationale (방법):

FOSS 에 공개적으로 Contribution 하는 것과 관련한 정책 개발을 위해 조직이 합당한 고려를 하였는지 확인한다. FOSS Contribution 정책은 조직의 전체 FOSS 정책의 일부로 만들 수도 있고, 자체적인 별도의 정책으로 만들 수도 있다. Contribution 이 전혀 허용되지 않는 상황이라면, 이를 명확히 하는 정책이 있어야 한다.

5.2 FOSS Contribution 정책이 Contributiond 을 허용하는 경우, Contribution 이 FOSS Contribution 정책을 준수하는지 확인하기 위한 Process 가 존재한다. 여기에는 다음과 같은 고려사항이 포함될 수 있지만, 이에 국한되지는 않는다:

- **License 고려에 대한 법적 승인**
- **사업상의 근거 또는 승인**
- **Contribution 할 Code 의 기술적 검토**
- **Community 참여 및 소통 (Project 의 행동 강령 혹은 이와 동등한 내용 포함)**
- **Project 별 Contribution 요구사항 준수**

Verification Artifact(s) (결과물 확인):

- 5.2.1 FOSS Contribution 정책이 Contribution 을 허용한다면, FOSS Contribution Process 를 설명하는 문서로 만들어진 절차가 존재한다.

Rationale (방법):

조직이 공개적으로 FOSS 에 Contribution 하는 방법에 대한 문서로 만들어진 Process 가 있는지 확인한다. Contribution 을 전혀 허용하지 않는 정책이 있을 수도 있다. 이러한 특정 상황에서는 Process 가 존재하지 않을 수 있으며, 그럼에도 이 요구사항은 충족되는 것이다.

G6: OpenChain 요구사항을 준수하는지 인증하라

6.1 조직이 OpenChain 인증을 받으려면, OpenChain Conformance Specification version 1.0 의 기준을 충족하는 FOSS Program 이 있음을 확약해야 한다.

Verification Artifact(s) (결과물 확인):

」 6.1.1 조직은 이 OpenChain Conformance Specification version 1.0 의 모든 요구 사항을 충족하는 Program 이 존재함을 확약한다.

Rationale (방법):

OpenChain Conforming 하는 Program 이 조직에 있음을 선언한다면, 해당 Program 이 이 specification 의 요구사항을 모두 충족하는지 확인한다. 이 요구사항의 일부만을 단순히 충족하는 것은 OpenChain 인증 Program 을 보증하기에 충분하지 않을 수 있다.