

OpenChain 준수 설명서

버전 1.0

목차

제 1 절 소개	4
제 2 절 정의	6
제 3 절 요구사항.....	7
G1: 당신의 FOSS 책임을 이해하라	7
G2: Compliance 달성을 위한 책임을 할당하라	9
G3: FOSS 내용을 검토하고 승인하라	10
G4: FOSS 내용 문서작성 및 결과물을 제공하라	11
G5: FOSS Community 참여를 이해하라	12
G6: OpenChain 요구사항 준수를 인증하라	13

면책

이 문서는 OpenChain Project 의 공식 번역본입니다. 원본인 영문 문서가 번역되었습니다. 번역본과 영문본 사이에 불일치가 있는 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.

저작권과 라이선스

Copyright © 2016 Linux Foundation. 본 설명서는 크리에이티브 커먼즈 애트리뷰션 라이선스 4.0(CC-BY-4.0)에 따라 이용허락됩니다. 그 라이선스의 사본은 여기서 얻을 수 있습니다: [CC-BY-4.0](https://creativecommons.org/licenses/by/4.0/)

제 1 절 소개

OpenChain Initiative 는 2013 년, 소프트웨어 공급망 오픈소스 전문가 그룹이 다음과 같은 두 가지 새로운 패턴을 관찰하면서 시작되었다. : 1) 성숙한 오픈소스 Compliance 프로그램이 있는 조직 간에는 중요한 절차적 유사성이 존재함; 2) 덜 발달된 프로그램을 가진, 소프트웨어를 교환하는 조직도 여전히 많이 존재하고 있음. 여기에서 두 번째 패턴은 소프트웨어 교환 시 동봉해야 하는 Compliance 결과물의 일관성 및 품질에 대한 신뢰가 결여되게 되었다. 결과적으로 소프트웨어 공급망 내 각 단계에서의 하위 조직은 상위 조직에서 이미 수행한 Compliance 작업을 다시 수행하는 일이 자주 발생하게 되었다.

이에 다음의 역할을 하는 표준적 프로그램 설명서가 제작될 수 있는지 검토하기 위해 스터디 그룹이 구성되었다: i) 업계에서 공유되는 오픈소스 Compliance 정보의 품질과 일관성 향상; ii) Compliance 재작업으로 인해 발생하는 높은 오픈소스 관련 거래 비용의 절감. 이 스터디 그룹은 워크 그룹으로 발전하였으며, 2016 년 4 월에는 Linux Foundation Collaborative Project 로 정식 조직되었다.

OpenChain Initiative 의 비전과 사명은 다음과 같다:

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

비전과 사명에 따라 이 설명서 일련의 요구사항을 정의하고, 이 요구사항을 충족하는 오픈소스 프로그램이라면 충분한 수준의 품질, 일관성 및 완전성을 달성했을 가능성을 높일 것이다. 다만, 설명서의 모든 요구사항을 만족하는 프로그램이라도 완전한 Compliance 가 보장되는 것은 아니다. 이 요구사항은 프로그램이 OpenChain 을 준수하는 것으로 인정하기 위해 충족해야 하는 기본 수준 (최소) 요구사항들을 의미한다. 이 설명서는 "어떻게"와 "언제"에 대한 고려가 아닌 Compliance 프로그램의 "무엇"과 "왜"에 대해 초점을 맞추고 있다. 이는 서로 다른 조직이 각자의 목적에 가장 잘 부합하도록 정책과 프로세스를 조정할 수 있게 하는 실질적인 유연성을 보장한다.

제 2 절에서는 설명서 전체에 걸쳐서 사용되는 주요 용어의 정의를 소개한다. 제 3 절에서는 각

v 2016 d

설명서 요구사항을 나타내는데, 각 요구사항에 대해 하나 혹은 그 이상의 검증 결과물 목록을 제시한다. 이들은 어떤 요구사항이 충족된 것으로 인정되기 위해 필요한 증거이다. 어떤 프로그램이 모든 요구사항을 충족한다면, 그 프로그램은 이 설명서 버전 1.0 에 따라 OpenChain 준수 프로그램으로 인정될 것이다.

제 2 절 정의

배포할 Compliance 결과물 - 식별된 라이선스가 공급대상 소프트웨어와 함께 제공하기를 요구하는 결과물의 집합. 여기에는 다음 사항이 포함된다 (이에 국한되지 않음). : 저작권 고지, 라이선스 사본, 수정 내용 고지, 저작자 고지, 소스 코드, 서면 청약 등

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

FOSS 연락담당자 - 외부로부터의 FOSS 문의를 받도록 지정된 사람.

식별된 라이선스 - 해당 라이선스를 식별하기 위한 적절한 방법을 수행한 결과로 식별된 FOSS 라이선스의 집합.

OpenChain 준수 프로그램 - 이 설명서의 모든 요구사항을 충족하는 프로그램.

소프트웨어 공급 담당자 - 공급대상 소프트웨어를 정의하거나, 그에 기여하거나 그를 준비하는 책임을 지는 모든 직원 또는 수급인. 조직에 따라 소프트웨어 개발자, 배포 엔지니어, 품질 엔지니어, 제품 마케팅 및 제품 관리자가 포함될 수 있지만, 이에 국한되지 않는다.

SPDX (Software Package Data Exchange) - 소프트웨어 패키지에 대한 라이선스 및 저작권 정보를 교환하기 위해 SPDX 워킹 그룹이 만든 표준 형식이다. SPDX 설명서에 대한 설명은 www.spdx.org 에서 확인할 수 있다.

공급대상 소프트웨어 - 한 조직에서 제 3 자(예: 다른 조직 혹은 개인)에게 제공(인도, 양도)하는 소프트웨어.

검증 결과물 - 주어진 요구사항을 충족한 것으로 판단하기 위해 존재해야 하는 증거.

제 3 절 요구사항

G1: 당신의 FOSS 책임을 이해하라

- 1.1 공급 대상 소프트웨어 배포 시에 필요한 FOSS 라이선스 Compliance 를 규정하고 최소한 내부에서 소통되어야 하는 문서화된 FOSS 정책이 존재한다.

검증 결과물:

- └ 1.1.1 문서화된 FOSS 정책이 존재한다.
- └ 1.1.2 모든 소프트웨어 공급담당자가 FOSS 정책의 존재를 인식하게 하는 문서화된 절차(예: 교육, 내부 wiki 혹은 기타 실질적인 의사소통 방법)가 존재한다.

이유:

FOSS 정책을 수립 및 기록하고 이를 소프트웨어 공급담당자가 인식하게 하는 조치가 취해지도록 보장하기 위함. 이 절에서는 정책에 포함되어야 할 요구사항이 규정되지 않지만, 다른 절에서 정책에 요구사항을 부과할 수도 있다.

- 1.2 모든 소프트웨어 공급담당자를 대상으로 다음과 같은 필수 FOSS 교육이 존재한다:

- 교육은 최소한 다음 주제를 다룬다:
 - FOSS 정책 및 사본을 찾을 수 있는 곳 ;
 - FOSS 및 FOSS 라이선스에 관한 지적재산법의 기본 ;
 - FOSS 라이선싱 개념 (Permissive 및 Copyleft 라이선스 개념 포함);
 - FOSS 프로젝트 라이선싱 모델 ;
 - 세부적인 FOSS Compliance 및 전반적인 FOSS 정책에 관한 소프트웨어 공급담당자의 역할 및 책임 ;
 - 공급 대상 소프트웨어에 포함된 FOSS Component 의 식별, 기록 및 추적을 위한 프로세스.
- 소프트웨어 공급담당자는 최근 24 개월 내 FOSS 교육을 이수하였어야 한다('현재 교육이수상태'). 소프트웨어 공급담당자가 교육 요구사항을 충족하도록 하기 위해 테스트할 수 있다.

검증 결과물:

- └ 1.2.1 위의 주제를 다루는 FOSS 과정 자료(예: 슬라이드 자료, 온라인 과정 혹은 이외 교육 자료)가 존재한다.
- └ 1.2.2 모든 소프트웨어 공급담당자가 과정을 완료하였는지 추적하는 방법.
- └ 1.2.3 적어도 소프트웨어 공급담당자의 85%가 현재 교육이수 상태(위 정의됨).

이유:

소프트웨어 공급관리자가 최근 FOSS 교육에 참석하고 FOSS 교육이 핵심 FOSS 주제를 다루도록 보장하기 위함. 의도는 핵심 기본 수준의 주제가 포함되도록 하기 위한 것이지만 일반적인 교육 프로그램은 여기에서 요구되는 것보다 더 포괄적 일 수 있다.

G2: Compliance 달성을 위한 책임을 할당하라

2.1 FOSS 연락담당자의 역할("FOSS 연락담당자")을 정한다.

- FOSS 관련 외부 문의 접수를 책임질 담당자를 지정한다;
- FOSS 연락담당자는 FOSS Compliance 문의에 적절히 대응하기 위해 상업적으로 합리적인 노력을 해야 한다; 그리고
- 전자 통신을 통해 FOSS 연락담당자에게 연락할 방법을 정해서 공개한다.

검증 결과물:

- └ 2.1.1 FOSS 연락담당자의 역할이 공개적으로 확인된다. (예: 이메일주소 및/또는 Linux Foundation 의 Open Compliance Directory 를 통해).
- └ 2.1.2 FOSS Compliance 문의의 접수 책임을 할당한 문서화된 절차가 존재한다.

이유:

제 3 자가 FOSS Compliance 문의와 관련하여 조직에 연락할 수 있는 합리적인 방법이 유지되도록 보장하기 위함.

2.2 FOSS Compliance 내부 담당자(들)을 지정한다.

- 내부 FOSS Compliance 를 관리할 개인을 지정한다. FOSS Compliance 담당자와 FOSS 연락담당자는 동일 개인이 될 수 있다.
- FOSS Compliance 관리 활동에는 충분한 자원이 공급된다:
- 역할을 수행할 시간이 배정된다; 그리고
- 상업적으로 합리적인 예산이 배정된다.
- FOSS 정책 및 프로세스를 개발하고 유지할 책임을 할당한다;
- FOSS Compliance 담당자는 FOSS Compliance 에 대한 (내외부) 법률 전문 지식에 접근할 수 있다; 그리고
- FOSS Compliance 이슈의 해결을 위한 긴급대응절차가 있다.

검증 결과물:

- └ 2.2.1 지정된 FOSS Compliance 담당자들, 조직 혹은 직무 이름.
- └ 2.2.2 FOSS Compliance 담당자가 사용할 수 있는 법률 전문 지식의 제공처를 지정한다.
- └ 2.2.3 FOSS Compliance 에 대한 책임을 할당한 문서화된 절차가 존재한다.
- └ 2.2.4 이슈 해결을 위한 긴급대응절차를 확인하는 문서화된 절차가 존재한다.

이유:

FOSS 책임이 효과적으로 할당되도록 보장하기 위함.

G3: FOSS 내용을 검토하고 승인하라

- 3.1 공급대상 소프트웨어에 포함된 모든 FOSS Component 들(및 그 각각 식별된 라이선스)을 확인, 추적 및 보관하는 프로세스가 존재한다.

검증 결과물:

- └ 3.1.1 공급대상 소프트웨어에 포함된 FOSS Component 들 및 그 식별된 라이선스 목록을 확인, 추적, 보관하는 문서화된 절차가 존재한다.

이유:

공급대상 소프트웨어를 제작하기 위해 사용된 모든 FOSS Component 들을 확인 및 목록화하기 위한 프로세스가 존재하도록 보장하기 위함. 이 목록은 공급대상 소프트웨어에 적용되는 배포 의무 및 제한 사항을 이해하기 위해 각 Component 의 라이선스 조항을 체계적으로 검토 할 수 있도록 존재해야 한다. 이 기록된 목록은 프로세스가 수행되었다는 증거로도 사용된다.

- 3.2 FOSS 프로그램은 공급대상 소프트웨어에 대해 소프트웨어 공급관리자가 접하게 되는 일반적인 FOSS 사용 사례를 처리할 수 있어야 하고, 사용 사례는 공급대상 소프트웨어의 일부가 다음 각 호에 해당할 경우를 포함할 수 있다(아래 각호가 모든 경우를 포함하지는 않으며 조직에 따라 아래의 모든 사항이 적용되는 것은 아님).:

- 바이너리 형태로 배포되는 경우
- 소스 형태로 배포되는 경우
- 다른 FOSS 와 통합되어 Copyleft 의무를 발생시키는 경우
- 수정한 FOSS 를 포함하는 경우
- 공급 대상 소프트웨어 내의 다른 Component 와 상호 작용하는, 상호충돌하는 라이선스가 적용되는 FOSS 혹은 다른 소프트웨어를 포함하는 경우
- 저작자 표시 요구사항이 있는 FOSS 를 포함하는 경우

검증 결과물:

- └ 3.2.1 공급대상 소프트웨어에 대해 소프트웨어 공급관리자가 만나게 되는 전형적인 FOSS 사용 사례를 처리할 수 있는 프로세스가 구현되었다.

이유:

해당 조직의 사업 실무의 결과로, FOSS 프로그램이 전형적인 사용 사례를 다루기에 충분히 견고하도록 보장하기 위함.

G4: FOSS 내용 문서작성 및 결과물을 제공하라

4.1 해당 식별된 라이선스에서 요구하는 대로 공급대상 소프트웨어와 함께 제공하기 위한 다음과 같은 배포할 Compliance 결과물(다음에 국한되지 않음)을 준비한다:

- 저작권 고지
- 식별된 라이선스의 사본
- 수정 내용 고지
- 저작자 고지
- 눈에 띄는 고지
- 소스 코드
- 요구되는 빌드 방법 및 스크립트
- 서면 청약

검증 결과물:

- ┌ 4.1.1 식별된 라이선스에서 요구하는대로 공급대상 소프트웨어와 함께 배포할 Compliance 결과물이 배포되도록 보장하는 프로세스를 설명하는 문서화된 절차가 존재한다.
- ┌ 4.1.2 배포할 Compliance 결과물의 사본이 보관되어 쉽게 검색할 수 있다 (예: 법적 고지, 소스 코드, SPDX 문서). 보관된 자료는 적어도 공급대상 소프트웨어가 제공되는 한 혹은 식별된 라이선스에서 요구하는 기한 동안 존재할 예정이다 (둘 중 더 긴 것을 따름).

이유:

공급대상 소프트웨어에 적용되는 식별된 라이선스에서 요구하는 대로 완전한 Compliance 산출물 집합이 공급대상 소프트웨어와 함께 제공되도록 보장하기 위함.

G5: FOSS 커뮤니티참여를 이해하라

- 5.1 조직을 대신하여 직원이 공개적으로 접근할 수 있는 FOSS 프로젝트에 기여하는 것을 규정하는 문서화된 정책이 존재하고 그 정책이 최소한 내부적으로 전파되어야 한다.

검증 결과물:

- └ 5.1.1 문서화된 FOSS 기여 정책이 존재한다;
- └ 5.1.2 모든 소프트웨어 공급담당자가 FOSS 기여 정책의 존재를 알도록 하는 문서화된 절차(예: 교육, 내부 wiki, 혹은 다른 실제적인 의사소통 방법을 통해)가 존재한다.

이유:

FOSS 에 공개적으로 기여 하는 것과 관련한 정책 개발을 위해 조직이 합당한 고려를 하도록 보장하기 위함. FOSS 기여 정책은 조직의 전체 FOSS 정책의 일부로 만들 수도 있고, 자체적인 별도의 정책으로 만들 수도 있다. 기여가 전혀 허용되지 않는 상황이라면, 이를 명확히 하는 정책이 있어야 한다.

- 5.2 FOSS 기여 정책이 이러한 기여 활동을 허용하는 경우, 다음을 포함하는 (그러나 이에 국한되지는 않는) FOSS 기여 정책을 준수하는지 확인하기 위한 프로세스가 존재한다:

- 라이선스 고려 사항에 대한 법적 승인
- 사업상의 근거 또는 승인
- 기여 할 코드의 기술적 검토
- 프로젝트의 행동 강령 또는 이와 동등한 내용을 포함하여 커뮤니티 참여 및 상호 작용
- 프로젝트별 기여 요구사항 준수

검증 결과물:

- └ 5.2.1 FOSS 기여 정책이 이러한 기여 활동을 허용하는 경우, FOSS 기여 절차를 설명하는 문서화된 프로세스가 존재한다.

이유:

공개적으로 FOSS 에 기여하는 방법에 대한 문서화된 프로세스를 조직이 갖도록 보장하기 위함. 기여가 전혀 허용되지 않는 정책이 있을 수도 있다. 이러한 특정 상황에서는 어떤 프로세스도 존재하지 않을 수 있으며, 그럼에도 이 요구사항은 충족되는 것이다.

G6: OpenChain 요구사항 준수를 인증하라

- 6.1 조직이 OpenChain 인증을 받으려면, OpenChain 준수 설명서 1.0 버전의 기준을 충족하는 FOSS 프로그램이 있음을 확약해야 한다.

검증 결과물:

- └ 6.1.1 조직은 이 OpenChain 준수 설명서의 모든 요구 사항을 충족하는 프로그램이 존재함을 확약한다.

이유:

조직이 OpenChain 을 준수하는 프로그램을 가지고 있다고 선언하면, 해당 프로그램이 이 설명서의 모든 요구사항을 충족하도록 보장하기 위함. 이 요구사항의 일부만을 충족하는 것만으로는 그 프로그램이 OpenChain 인증된 것으로 보증하기에 충분하지 않을 것이다.