OPENCHAIN

OpenChain 설명서

버전 1.2

목차

면책

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

저작권과 라이선스

1) 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 컴플라이언스 프로그램이 있는 조직 간에는 중요한 절차적 유사성이 존재함; 2) 덜 발달된 프로그램으로 소프트웨어를 거래하는 조직도 여전히 많이 존재하고 있음. 여기에서 두 번째 패턴은 소프트웨어 거래 시 수반하는 컴플라이언스 결과물의 일관성 및 품질에 대한 신뢰가 결여되는 결과를 가져왔다. 결과적으로 소프트웨어 공급망 내 각 단계에서의 하위 조직은 상위 조직에서 이미 수행한 컴플라이언스 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 컴플라이언스 정보의 품질과 일관성 향상; ii) 컴플라이언스 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 컴플라이언스 정보와 함께 Free/Open Source Software(FOSS)를 제공하는 소프트웨어 공급망
- **사명**: 소프트웨어 공급망 참가자를 위해, FOSS 의 효과적인 관리를 위한 요건을 수립하여 요건 및 부수적인 관련 사항을 소프트웨어 공급망, 오픈소스 커뮤니티 및 학계의 대표들이 공동으로 그리고 공개적으로 개발할 수 있도록 한다.

비전과 사명에 따라 이 설명서 일련의 요건을 정의하고, 이 요건을 충족하는 오픈소스 프로그램이라면 충분한 수준의 품질, 일관성 및 완전성을 달성했을 가능성을 높일 것이다. 다만, 설명서의 모든 요건을 만족하는 프로그램이라도 완전한 컴플라이언스가 보장되는 것은 아니다. 이 요건은 프로그램이 OpenChain 을 준수하는 것으로 인정하기 위해 충족해야 하는 기본 수준 (최소) 요건들을 의미한다. 이 설명서는 "어떻게"와 "언제"에 대한 고려가 아닌 컴플라이언스 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 설명서 요건을 나타내는데, 각 요건에 대해 하나 혹은 그 이상의 검증 자료를 제시한다. 이들은 어떤 요건이 충족된 것으로 인정되기 위해 필요한 증거이다. 만약 어떤 프로그램이 모든 요건을 충족한다면, 그 프로그램은 이 설명서 버전 1.2 에 따라 OpenChain 준수 프로그램으로 인정될 것이다. 검증 자료는 공개용으로 작성된 것은 아니지만, 준수를 인증하기 위해 NDA(비공개합의) 하에서 또는 OpenChain 조직의 개별적 요청에 따라 제공될 수 있다.

설명서를 해석하는 방법에 대한 추가 설명은 다음 위치에 있는 설명서 FAQ(자주 묻는 질문)를 검토하여 얻을 수 있다 :
https://www.openchainproject.org/specification-faq

2) 제 2 절 정의

컴플라이언스 결과물 – 공급 대상 소프트웨어 배포에 대한 FOSS 관리 프로그램의 산출물을 나타내는 결과물 집합 이 집합에는 다음 중 하나 이상이 포함될 수 있다 (단, 이에 국한되지 않음): 소스 코드, 저작자 고지, 저작권 고지, 라이선스 사본, 수정 내용 고지, 서면 청약, FOSS 컴포넌트 BOM (bill of materials), SPDX 문서 등.

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

FOSS 연락담당자 – 외부로부터의 FOSS 문의를 받도록 지정된 사람.

식별된 라이선스 – 공급대상 소프트웨어에 적용되는 라이선스를 식별하기 위한 적절한 방법을 수행한 결과로 식별된 일련의 FOSS 라이선스

OpenChain 준수 프로그램–**이 설명서의 모든 요건을 충족하는 프로그램.**

소프트웨어 공급 담당자 – 공급대상 소프트웨어의 범위를 정의하거나, 그 소프트웨어에 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 자료 – 주어진 요건이 충족되는 것으로 인정되기 위해 존재해야 하는 증거.

3) 제 3 절 요건

목표 1: FOSS 책임 파악

1.1 **공급 대상 소프트웨어 배포 시에 필요한 FOSS 라이선스 컴플라이언스를 규정하는 문서화된 FOSS 정책이 존재한다.** 이 정책은 내부적으로 전달되어야 한다.

검증 자료

1.1.1 문서화된 정책.

1.1.2 모든 소프트웨어 공급담당자가 FOSS 정책의 존재를 인식하게 하는 문서화된 절차(예: 교육, 내부 wiki 혹은 기타 실질적인 의사소통 방법)

이유:

FOSS 정책을 수립 및 기록하고 이 존재를 소프트웨어 공급담당자가 인식하게 하는 조치가 취해지도록 보장하기 위함. 이 절에서는 정책에 포함되어야 할 요건이 규정되지 않지만, 다른 절에서 정책에 요건을 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 지식재산권법의 기본;**
  - **FOSS 라이선싱 개념 (Permissive 및 Copyleft 라이선스 개념 포함);**
  - **FOSS 프로젝트 라이선싱 모델;**
  - **세부적인 FOSS 컴플라이언스 및 전반적인 FOSS 정책에 관한 소프트웨어 공급담당자의 역할 및 책임**
  - **공급 대상 소프트웨어 포함된 FOSS Component 의 식별, 기록 및 추적을 위한 프로세스.**
- **소프트웨어 공급담당자는 현재 교육 이수 상태로 인정되기 위해서 지난 24 개월 내 FOSS 교육을 이수하였어야 한다('현재 교육 이수 상태'). 소프트웨어 공급담당자가 교육 요건을 충족할 수 있도록 하기 위해 테스트가 행해질 수 있다.**

검증 자료

1.2.1 위의 주제를 다루는 FOSS 교육 자료(예: 슬라이드 자료, 온라인 과정 혹은 이외 교육 자료)

1.2.2 소프트웨어 공급담당자가 교육을 완료하였는지 추적하는 문서화된 방법.

1.2.3 소프트웨어 공급담당자의 85% 이상이 위의 정의에 따라 현재 교육 이수 상태 85%는 반드시 전체 조직을 지칭하는 것이 아니고, OpenChain 준수 프로그램이 적용되는 전체 소프트웨어 공급담당자를 지칭할 수 있다.

이유:

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

1.3 **각 라이선스가 부여하는 의무, 제한 및 권리를 결정하기 위해 식별된 라이선스를 검토하는 프로세스가 존재한다.**

검증 자료

1.3.1 식별된 각 라이선스에 의해 부과되는 의무, 제한 및 권리를 검토하고

문서화하기 위한 문서화된 절차

이유:

다양한 사용 사례에 대해 각 식별된 라이선스에 대한 라이선스 의무를 검토하고 식별하기 위한 프로세스가 존재하도록 보장하기 위함.

목표 2: 컴플라이언스 달성을 위한 책임 할당

2.1 외부 FOSS 연락담당자의 역할을 정한다.

- FOSS 관련 외부 문의 접수를 책임질 담당자를 지정한다;
- FOSS 연락담당자는 FOSS 컴플라이언스 문의에 적절히 대응하기 위해 상업적으로 합리적인 노력을 해야 한다; 그리고
- FOSS 연락담당자에게 연락할 수 있는 방법을 공개적으로 밝힌다.

검증 자료

2.1.1 공개적으로 식별 가능한 FOSS 연락담당자의 ID (예: 공개된 이메일 주소, 또는 Linux Foundation 의 Open Compliance Directory.)

2.1.2 FOSS 컴플라이언스 문의의 접수 책임을 할당하는 내부 문서화된 절차

이유:

FOSS 컴플라이언스 문의와 관련하여 제 3 자가 조직에 연락할 수 있는 합리적인 방법이 있고, 이 책임이 효과적으로 할당되도록 보장하기 위함.

2.2 FOSS 컴플라이언스 내부 담당자(들)를 지정한다.

- 내부 FOSS 컴플라이언스를 관리할 개인을 지정한다. FOSS 컴플라이언스 담당자와 FOSS 연락담당자는 동일 개인이 될 수 있다.
- FOSS 컴플라이언스 관리 활동에는 충분한 자원이 공급된다:
  - 역할을 수행할 시간이 배정된다; 그리고
  - 상업적으로 합리적인 예산이 배정된다.
- FOSS 정책 및 프로세스를 개발하고 유지할 책임을 할당한다;
- FOSS 컴플라이언스 담당자는 FOSS 컴플라이언스에 대한 (내외부) 법률 전문 지식을 이용할 수 있다; 그리고
- FOSS 컴플라이언스 이슈의 해결을 위한 프로세스가 존재한다.

검증 자료

2.2.1 내부적으로 지정된 FOSS 컴플라이언스 담당자, 조직 혹은 직무 이름.

2.2.2 FOSS 컴플라이언스 담당자가 사용할 수 있는 내부 또는 외부의 법률 전문 지식의 식별

2.2.3 FOSS 컴플라이언스를 위한 내부 책임을 할당하는 문서화된 절차

2.2.4 미준수 사례의 검토 및 시정을 규정하는 문서화된 절차

이유:

FOSS 책임이 효과적으로 할당되도록 보장하기 위함.

목표 3: FOSS 내용 검토 및 승인

3.1 **공급대상 소프트웨어 내의 각 Component(및 그 식별된 라이선스)를 포함하는 FOSS Component 목록(BOM)을 작성하고 관리하는 프로세스가 존재한다.**

검증 자료

3.1.1 공급대상 소프트웨어 배포판에 포함되어 있는 FOSS Component 들 집합에 대한 정보를 식별, 추적 및 보관하기 위한 문서화된 절차.

3.1.2 문서화된 절차가 각 공급 대상 소프트웨어 배포판에 대해 올바르게 수행되었음을 입증하는 FOSS Component 기록

이유:

공급대상 소프트웨어를 제작하기 위해 사용된 FOSS 구성목록(BOM)을 작성하고 관리하기 위한 프로세스가 존재하도록 보장하기 위함. 공급대상 소프트웨어의 배포에 적용되는 의무와 제한 사항을 이해하기 위해 각 Component 의 라이선스 조항에 대한 체계적 검토를 지원하려면 BOM 이 필요하다.

3.2 **FOSS 관리 프로그램은 공급대상 소프트웨어에 대해 소프트웨어 공급관리자가 접하게 되는 일반적인 FOSS 라이선스 사용 사례를 처리할 수 있어야 하며, 다음과 같은 사용 사례가 포함될 수 있다. (아래 각호가 모든 경우를 포함하지는 않으며, 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 작용하면서 양립 불가능한 라이선스가 적용된 FOSS 혹은 다른 소프트웨어를 포함하는 경우;**
- **저작자 표시 요건이 있는 FOSS 를 포함하는 경우.**

검증 자료

3.2.1 각 공급대상 소프트웨어 배포판의 FOSS Component 에 대한 일반적인 FOSS 라이선스 사용 사례를 다루는 서면화된 절차

이유:

FOSS 관리 프로그램이 조직의 일반적인 FOSS 라이선스 사용 사례들을 처리할 수 있을만큼 충분히 견고함을 보장하기 위함. 이 활동을 지원하기 위한 절차가 존재하고 그 절차가 준수되는지를 보장하기 위함.

목표 4: FOSS 내용 문서 및 결과물 제공

4.1 각 공급 대상 소프트웨어에 대해 컴플라이언스 결과물 세트를 작성하기 위한 프로세스가 존재한다.

검증 자료

4.1.1 식별된 라이선스에서 요구하는 대로 컴플라이언스 결과물이 준비되어서 공급 대상 소프트웨어와 함께 배포되도록 보장하는 문서화된 절차.

4.1.2 공급 대상 소프트웨어 배포판의 컴플라이언스 결과물 사본이 보관되어 쉽게 다시 검색할 수 있으며, 보관된 자료는 적어도 공급대상 소프트웨어가 제공되는 한 혹은 식별된 라이선스에서 요구하는 기한 동안 제공된다(둘 중 더 긴 것을 따름).

이유:

식별된 라이선스에 따라 요구되는 컴플라이언스 결과물의 집합이 FOSS 검토 프로세스의 일부로 작성된 기타 보고서와 함께 공급대상 소프트웨어에 수반하도록 보장하기 위함.

목표 5: FOSS 커뮤니티 참여 이해

5.1 조직이 FOSS 프로젝트에 기여하는 것을 관리하는 문서화된 정책이 존재한다. 이 정책은 내부적으로 전달되어야 한다.

검증 자료

5.1.1 문서화된 FOSS 기여 정책;

5.1.2 모든 소프트웨어 공급담당자가 FOSS 기여 정책의 존재를 알도록 하는 문서화된 절차(예: 교육, 내부 wiki, 혹은 다른 실제적인 의사소통 방법을 통해).

이유:

FOSS 에 대한 공개적 기여와 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 제한적이거나, 전혀 허용되지 않는 상황이라면, 이를 명확히 하는 정책이 있어야 한다.

5.2 FOSS 프로젝트에 기여하는 것을 허용하는 조직이라면 5.1 절에 설명한 FOSS 기여 정책을 구현하는 프로세스가 존재한다.

검증 자료

5.2.1 FOSS 기여 정책이 기여를 허용하는 경우, FOSS 기여를 관리하는 문서화된 절차.

이유:

공개적으로 FOSS 에 기여하는 방법에 대한 문서화된 프로세스를 조직이 갖도록 보장하기 위함. 기여가 전혀 허용되지 않는 정책이 있을 수도 있다. 그런 상황에서는 어떠한 절차도 존재하지 않을 수 있으며, 그럼에도 이 요건은 충족된 것으로 이해된다.

목표 6: OpenChain 요건 준수 인증

6.1 조직이 OpenChain 인증을 받으려면, OpenChain 설명서 1.2 버전의 기준을 충족하는 FOSS 관리 프로그램이 있음을 확약해야 한다.

검증 자료

6.1.1 이 OpenChain 1.2 버전의 모든 요건을 충족하는 FOSS 관리 프로그램의 존재 확약.

이유:

조직이 OpenChain 을 준수하는 프로그램을 가지고 있다고 선언하면, 해당 프로그램이 이 설명서의 모든 요건을 충족하였음을 보장하기 위함. 이러한 요건의 일부를 충족하는 것 만으로는 충분하다고 인정되지 않는다.

6.2 이 설명서 버전의 준수는 준수 인증이 이루어진 날로부터 18 개월 동안 지속된다. 준수 인증 요건은 OpenChain 프로젝트의 웹 사이트에서 찾을 수 있다.

검증 자료

6.2.1 조직은 준수 인증을 받은 후 18 개월 동안 이 OpenChain 설명서 1.2 버전의 모든 요건을 충족하는 FOSS 관리 프로그램이 존재함을 확약한다.

이유:

조직이 시간이 지난 후에도 프로그램 준수를 주장하고자 한다면 현재에도 설명서가 조직에서 통용되는 것이 중요. 이 요건은 준수 조직이 시간이 지나도 계속해서 준수를 주장하는 경우 프로그램의 지원 프로세스와 통제가 약화되지 않았음을 보장하기 위함.

부록 I: 언어 번역

글로벌 채택을 촉진하기 위해 설명서를 여러 언어로 번역하는 노력을 환영합니다. OpenChain 은 오픈소스 프로젝트로서의 기능을 수행하기 때문에 번역은 CC-BY 4.0 라이선스 및 프로젝트의 번역 정책에 따라 번역을 수행하는데 시간과 전문 지식을 기꺼이 기여한 사람들에 의해 이루어집니다. 정책 및 사용 가능한 번역에 대한 자세한 내용은 OpenChain 프로젝트 설명서 웹 페이지에서 확인할 수 있습니다.