OPENCHAIN

OPENCHAIN 설명서

Version 2.0

소프트웨어 솔루션을 구성하는 오픈소스에 대한 신뢰 구축

목차

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 this translation and the English version, The English text shall take precedence.

이 문서는 OpenChain Project 의 공식 번역본입니다. 영어 원문에서 번역되었습니다. 번역본과 영문본 사이에 불일치가 있는 경우, 영문본이 우선합니다.

1) 소개

이 설명서는 우수한 오픈소스 컴플라이언스 프로그램의 핵심 요건을 정의한다. 이 설명서의 목표는 오픈소스 소프트웨어로 구성된 소프트웨어 솔루션을 주고받는 조직 간에 신뢰를 구축하기 위한 기준을 제공하는 것이다. OpenChain 설명서를 준수한다고 인정받은 프로그램은 각 소프트웨어 솔루션에 대한 필수 컴플라이언스 결과물(법적 고지, 소스 코드 등)을 산출하도록 설계되었음을 보증한다. OpenChain 설명서는 프로그램의 "how"와 "when"이 아니라 "what"과 "why" 측면에 중점을 둔다. 이를 통해 각기 다른 시장의 서로 다른 규모의 여러 조직이 자신의 규모, 목표 및 범위에 맞는 특정 정책 및 프로세스 컨텐츠를 선택할 수 있는 유연성을 보장한다. 예를 들어, OpenChain 준수(Conformance) 프로그램은 단일 제품군 또는 전체 조직을 대상으로 적용 할 수 있다.

이 소개는 모든 잠재적 사용자를 위한 개요이다. 2 장 에서는 설명서 전체에서 사용되는 주요 용어를 정의한다. 3 장에서는 프로그램이 OpenChain 설명서를 준수하기 위해 충족해야 하는 요건을 정의한다. 하나의 요건은 이를 충족하기 위해 생성되어야 하는 하나 이상의 검증 자료(기록 등)로 구성된다. 검증 자료를 공개해야 할 필요는 없지만, 선택적으로 비공개 계약(NDA)하에 다른 조직에 제공할 수 있다.

설명서는 150 명 이상의 기여자로부터 피드백을 받은 오픈 이니셔티브로 개발되었다. 설명서 메일링 리스트와 자주하는 질문(FAQ)을 검토하면 개발 이력을 이해할 수 있다.

2) 정의

"컴플라이언스 결과물" - 공급 대상 소프트웨어에 대한 프로그램 산출물의 결과물 모음. 이 모음에는 다음 중 하나 이상이 포함될 수 있다 (단, 이에 국한되지 않음) : 소스 코드, 저작자 고지, 저작권 고지, 라이선스 사본, 수정 내용 고지, 서면 청약, 오픈소스 컴포넌트 BOM (Bill of Materials), SPDX 문서.

"식별된 라이선스" - 공급 대상 소프트웨어가 구성하는 오픈소스 컴포넌트를 식별하기 위한 적합한 방법을 따른 결과로 식별된 오픈소스 라이선스의 집합.

"OpenChain 준수(Conformant)" - 이 설명서의 모든 요건을 충족하는 프로그램.

"오픈소스" - Open Source Initiative(OpenSource.org)에서 발표한 Open Source Definition 혹은 Free Software Foundation 에서 발표한 Free Software Definition 을 충족하는 라이선스, 혹은 유사한 라이선스가 하나 이상 적용된 소프트웨어.

"**프로그램**" – 조직의 오픈소스 라이선스 컴플라이언스 활동을 관리하는 정책, 프로세스 및 담당자 집합.

"소프트웨어 공급 담당자" - 공급 대상 소프트웨어의 범위를 정의하거나, 기여 또는 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" - 특정 소프트웨어 패키지에 대한 라이선스 및 저작권 정보를 교환하기 위해 Linux Foundation 의 SPDX (Software Package Data Exchange) 워킹 그룹에서 작성한 형식 표준. SPDX 설명서에 대한 설명은 www.spdx.org 에서 확인할 수 있다.

"공급 대상 소프트웨어" - 조직이 제 3 자(다른 조직 또는 개인)에게 배포하는 소프트웨어.

"검증 자료" - 주어진 요건이 충족되었음을 입증하는 자료.

3) 요건

1.0 프로그램 설립

1.1 정책

공급 대상 소프트웨어의 오픈소스 라이선스 컴플라이언스를 관리하는 문서화된 오픈소스 정책이 존재한다. 정책은 내부적으로 전달되어야 한다.

검증 자료:

- 1.1.1 문서화된 오픈소스 정책.
- 1.1.2 소프트웨어 공급 담당자가 오픈소스 정책의 존재를 인식하도록 하는 문서화 된 절차 (교육, 내부 위키, 혹은 기타 실질적인 의사소통 방법 등).

이유:

오픈소스 정책을 생성 및 기록하고, 소프트웨어 공급 담당자가 오픈소스 정책을 확인할 수 있게 하기 위한 조치가 취해지는 것을 보장하기 위함. 정책에 포함되어야 요건은 다른 장에서 설명할 것임.

1.2 역량

조직은 다음 사항을 수행해야 한다:

- **프로그램의 성능 및 효과에 영향을 미치는 역할과 해당 역할에 대한 책임을 확인한다;**
- **각 역할을 수행하는 인원의 필요한 역량을 파악한다;**
- **해당 인원이 적절한 교육, 훈련 및 경험을 바탕으로 자격을 갖춘 자임을 보장한다;**
- **해당되는 경우, 필요한 역량을 확보하기 위한 조치를 취한다;**
- **적절히 문서화된 정보를 역량의 증거로 보유한다.**

검증 자료:

- 1.2.1 프로그램 내 여러 참여자에 대한 문서화된 책임과 역할 목록.
- 1.2.2 각 역할에 대한 역량을 확인하는 문서.
- 1.2.3 각 프로그램 참여자에 대해 역량을 평가한 문서화된 증거.

이유:

프로그램 역할을 수행하는 확인된 참여자가 각자의 역할과 책임에 대해 충분한 수준의 역량을 확보하도록 보장하기 위함.

1.3 인지도

조직은 프로그램 참여자가 다음 사항을 알고 있음을 보장해야 한다:

a) 오픈소스 정책;

b) 오픈소스 관련 목표;

c) 프로그램의 효과에 대한 기여;

d) 프로그램의 요건 미준수의 의미.

검증 자료:

- 1.3.1 각 프로그램 담당자에 대해 프로그램의 목표, 프로그램에 기여, 그리고 프로그램 미준수의 의미를 포함하는 인지도를 평가한 문서화된 증거.

이유:

프로그램 담당자가 프로그램 내에서 각자의 역할과 책임에 대해 충분한 수준의 인지도를 확보하도록 보장하기 위함.

1.4 프로그램 적용 범위

서로 다른 프로그램들은 서로 다른 수준의 범위까지 적용될 수 있다. 예를 들어, 하나의 프로그램이 하나의 제품 라인, 전체 부서 또는 전체 조직을 관리할 수 있다. 각 프로그램별로 범위 지정이 이루어질 필요가 있다.

검증 자료:

- 1.4.1 프로그램의 적용 범위와 한계를 명확하게 정의한 문서화된 진술.

이유:

조직의 필요 범위에 가장 적합한 프로그램을 구성할 수 있도록 유연성을 제공하기 위함. 일부 조직은 특정 제품군에 대해서만 프로그램을 유지하도록 선택할 수 있고 또한, 다른 조직은 전체 조직의 공급 대상 소프트웨어를 관리하도록 프로그램을 구현할 수 있다.

1.5 라이선스 의무

각 라이선스에 의해 부여된 의무, 제한 및 권리를 결정하기 위해 식별된 라이선스를 검토하는 프로세스가 존재한다.

검증 자료:

- 1.5.1 각 식별된 라이선스에 의해 부과되는 의무, 제한 및 권리를 검토하고 문서화하기 위한 문서화된 절차.

이유:
조직이 직면할 수 있는 다양한 사용 사례(요건 3.2 에 정의)에 대해 각 식별된 라이선스의 의무를 검토하고 확인하기 위한 프로세스가 존재하도록 보장하기 위함.

2.0 관련 태스크 정의 및 지원

2.1 접근성

외부 오픈소스 문의에 효과적으로 대응할 수 있는 프로세스를 유지한다. 제 3 자가 오픈소스 컴플라이언스 문의를 할 수 있는 방법을 공개적으로 밝힌다.

검증 자료:

- 2.1.1 제 3 자가 오픈소스 컴플라이언스 문의를 할 수 있게 공개적으로 알려진 방법 (공개된 연락처 이메일 주소, 또는 Linux Foundation 의 Open Compliance Directory 등).
- 2.1.2 제 3 자의 오픈소스 라이선스 컴플라이언스 문의에 대응하기 위한 내부의 문서화된 절차.

이유:

제 3 자가 오픈소스 컴플라이언스 문의를 위해 조직에 연락할 수 있는 합리적인 방법이 존재하고 조직이 효과적으로 대응할 준비가 되도록 보장하기 위함.

2.2 효과적인 리소스 제공

프로그램 업무를 확인하고 리소스를 제공하라:

- **프로그램 업무를 성공적으로 수행할 수 있도록 책임을 할당하라.**
- **프로그램 업무를 위해 충분한 리소스가 제공된다:**
  - **업무를 수행할 시간이 할당되었다;**
  - **적절한 자금이 할당되었다.**
- **정책 및 지원 업무를 검토하고 업데이트하는 프로세스가 존재한다;**
- **오픈소스 라이선스 컴플라이언스와 관련된 법률 가이드를 필요로 하는 인원이 법률 전문 지식을 이용할 수 있다;**
- **오픈소스 라이선스 컴플라이언스 문제를 해결하기 위한 프로세스가 존재한다.**

검증 자료:

- 2.2.1 확인된 프로그램 역할의 담당자 이름, 그룹 또는 기능이 기재된 문서.
- 2.2.2 확인된 프로그램 역할이 적절하게 충원되었고 적합하게 자금이 제공되었다.
- 2.2.3 오픈소스 라이선스 컴플라이언스 문제를 해결하기 위해 내부 또는 외부의 전문 법률 지식을 이용할 수 있는 방법의 확인.
- 2.2.4 오픈소스 컴플라이언스에 대한 내부 책임을 할당하는 문서화된 절차.
- 2.2.5 미준수 사례의 검토 및 시정을 규정하는 문서화된 절차.

이유:

i) 프로그램 책임이 효과적으로 지원되고 리소스를 제공받으며 ii) 정책 및 지원 프로세스가 새로운 오픈소스 컴플라이언스 모범 사례를 수용하기 위해 정기적으로 업데이트되는 것을 보장하기 위함.

3.0 오픈소스 콘텐츠 검토 및 승인

3.1 BOM (Bill of Materials)

공급 대상 소프트웨어를 구성하는 각 오픈소스 컴포넌트(및 식별된 라이선스)를 포함하는 BOM 을 작성하고 관리하는 프로세스가 있다.

검증 자료:

- ☐ 3.1.1 공급 대상 소프트웨어를 구성하는 오픈소스 컴포넌트 모음에 대한 정보를 식별, 추적, 검토, 승인 및 보관하는 문서화된 절차.
- ☐ 3.1.2 공급 대상 소프트웨어에 대해 문서화된 절차가 적절히 준수되었음을 입증하는 오픈소스 컴포넌트 기록.

이유:

공급 대상 소프트웨어를 구성하는데 사용된 오픈소스 컴포넌트 BOM 을 생성하고 관리하기 위한 프로세스가 존재함을 보장하기 위함. 공급 대상 소프트웨어의 배포에 적용되는 의무와 제한 사항을 이해하기 위해 각 컴포넌트의 라이선스 조건에 대한 체계적인 검토와 승인을 지원하는 BOM 이 필요하다.

3.2 라이선스 컴플라이언스

프로그램은 공급 대상 소프트웨어에 대해 소프트웨어 공급 담당자가 접하게 되는 일반적인 오픈소스 사용 사례를 처리할 수 있어야 하며, 다음과 같은 사례가 포함될 수 있다(이 목록이 완전한 것은 아니며, 모든 사용 사례가 적용되어야 하는 것은 아니다).:

- **바이너리 형태로 배포;**
- **소스 형태로 배포;**
- **Copyleft 의무를 발생시킬 수 있는 다른 오픈소스와 통합;**
- **수정한 오픈소스를 포함;**
- **공급 대상 소프트웨어 내에서 상호 작용하는 다른 컴포넌트와 호환되지 않는 라이선스 하의 오픈소스 또는 기타 소프트웨어를 포함;**
- **저작자 표시 요건이 있는 오픈소스를 포함.**

검증 자료:

- ☐ 3.2.1 공급 대상 소프트웨어의 오픈소스 컴포넌트에 대해 일반적인 오픈소스 라이선스 사용 사례를 처리하기 위한 문서화된 절차.

이유:

프로그램이 조직의 일반적인 오픈소스 라이선스 사용 사례를 처리하기에 충분히 견고하고, 이 활동을 지원하기 위한 절차가 존재하며 이 절차를 준수하도록 하기 위함.

4.0 컴플라이언스 결과물 생성 및 전달

4.1 컴플라이언스 결과물

공급 대상 소프트웨어에 대한 컴플라이언스 결과물 세트를 생성하는 프로세스가 존재한다.

검증 자료:

- 4.1.1 식별된 라이선스에서 요구하는 대로 컴플라이언스 결과물을 준비하고 공급 대상 소프트웨어와 함께 배포하기 위한 프로세스를 설명하는 문서화된 절차.

- 4.1.2 공급 대상 소프트웨어의 컴플라이언스 결과물 사본을 보관하기 위한 문서화된 절차 - 보관 파일은 공급 대상 소프트웨어의 마지막 제공 이후 적절한 기간(혹은 식별된 라이선스가 요구하는 기간 (둘 중 더 긴 시간)) 동안 보관되어야 한다. 절차가 올바르게 지켜졌음을 입증하는 기록이 존재한다.

이유:

식별된 라이선스가 요구하는 대로 공급 대상 소프트웨어와 함께 제공되는 컴플라이언스 결과물을 준비할 때 합리적인 상업적 노력이 이루어지도록 보장하기 위함.

5.0 오픈소스 커뮤니티 참여에 대한 이해

5.1 기여

조직이 오픈소스 프로젝트에 기여를 고려한다면

- **오픈소스 프로젝트에 대한 기여를 관리하는 문서화된 정책이 존재한다;**
- **이 정책이 내부적으로 전달되어야 한다;**
- **정책을 구현하는 프로세스가 존재한다.**

검증 자료:

조직이 오픈소스 프로젝트에 대한 기여를 허용한다면 다음이 존재해야 한다:

- 5.1.1 문서화된 오픈소스 기여 정책;
- 5.1.2 오픈소스 기여를 관리하는 문서화된 절차;
- 5.1.3 모든 소프트웨어 공급 담당자가 오픈소스 기여 정책의 존재를 인식하도록 하는 문서화된 절차 (교육, 내부 위키, 또는 기타 실질적인 의사소통 방법 등).

이유:

조직이 오픈소스 기여를 허용한다면 기여 정책을 개발하고 이행하는 데 있어 합리적인 고려를 하도록 보장하기 위함. 오픈소스 기여 정책은 전체 오픈소스 정책의 일부가 될 수도 있고 자체적인 별도의 정책일 수도 있다.

6.0 설명서 요건 준수

6.1 준수 (Conformance)

프로그램이 OpenChain 을 준수한다고 간주되려면 조직은 프로그램이 이 설명서에 제시된 요건을 충족하는지 확인해야 한다.

검증 자료:

- 6.1.1 요건 1.4 에 명시된 프로그램을 확인하는 문서는 이 설명서의 모든 요건을 충족한다.

이유:

조직이 OpenChain 을 준수하는 프로그램을 가지고 있다고 선언한 경우 해당 프로그램이 이 설명서의 모든 요건을 충족한다는 것을 보장하기 위함. 단순히 이 요건의 일부를 충족하는 것만으로는 충분하다고 볼 수 없다.

6.2 기간

이 설명서 버전에 대한 OpenChain 준수 프로그램은 준수한다고 확인이 이루어진 날로부터 18 개월동안 지속된다. 준수 확인 등록 절차는 OpenChain 프로젝트의 웹사이트에서 확인할 수 있다.

검증 자료:

- 6.2.1 준수한다는 확인이 이루어진 후 18 개월 이내에 이 설명서 버전(2.0)의 모든 요건을 충족하는 것을 확인하는 문서.

이유:

조직이 시간이 지난 후에도 프로그램이 준수한다고 주장하고자 한다면 조직은 현재에도 설명서대로의 요건을 보장하는 것이 중요하다. 이 요건은 조직이 시간이 지남에 따라 프로그램 준수를 계속 주장하는 경우 프로그램의 지원 프로세스와 통제가 약화되지 않았음을 보장한다.

부록 I: 언어 번역

국제 표준 채택을 용이하게 하기 위해 설명서를 다른 언어로 번역하려는 노력을 환영합니다. OpenChain 은 오픈소스 프로젝트로서 기능을 하기 때문에, 번역은 시간과 전문지식을 기꺼이 기부한 사람들에 의해 이루어집니다. 정책과 사용 가능한 번역의 자세한 내용은 OpenChain 프로젝트 설명서 웹페이지에서 확인할 수 있습니다.