OpenChain 규격
Version 2.1

이 규격은 기능적으로 다음과 동일하다

- **OpenChain 규격 2.0**
- **ISO/IEC PRF 5230**

자세한 내용은 www.openchainproject.org 참조

© Joint Development Foundation 2020 – 자세한 내용 및 자체 인증은 www.openchainproject.org 참조

목차

소개 iii

1 적용 범위 1

2 용어와 정의 1

3 요구사항 2

3.1 프로그램 설립 2

3.1.1 정책 2

3.1.2 역량 2

3.1.3 인식 3

3.1.4 프로그램 적용 범위 3

3.1.5 라이선스 의무 4

3.2 관련 업무 정의 및 지원 4

3.2.1 외부 문의 대응 (Access) 4

3.2.2 효과적인 리소스 제공 4

3.3 오픈소스 콘텐츠 검토 및 승인 5

3.3.1 BOM (Bill of Materials) 5

3.3.2 라이선스 컴플라이언스 5

3.4 컴플라이언스 산출물 생성 및 전달 6

3.4.1 컴플라이언스 산출물 6

3.5 오픈소스 커뮤니티 참여에 대한 이해 6

3.5.1 기여 6

3.6 규격 요구사항 준수 7

3.6.1 적합성 (Conformance) 7

3.6.2 지속 기간 7

부록 A (정보) 다국어 번역 8

 © Joint Development Foundation 2020 –자세한 내용 및 자체 인증은 www.openchainproject.org 참조

소개

이 문서는 우수한 오픈소스 라이선스 컴플라이언스 프로그램의 핵심 요구사항을 정의한다. 이 문서의 목표는 오픈소스로 구성된 소프트웨어 솔루션을 주고 받는 조직 간에 신뢰를 구축하기 위한 기준을 제공하는 것이다. OpenChain 규격에 적합하다고 인정된 프로그램은 각 소프트웨어 솔루션에 대해 필요한 컴플라이언스 산출물(법적 고지, 소스 코드 등)을 생성하도록 설계되었음을 보장한다. 이 문서는 프로그램의 "How"와 "When"보다는 "What"과 "Why" 측면에 중점을 둔다. 이를 통해 시장 규모에 따라 각기 다른 조직의 규모, 목표, 범위에 맞는 구체적인 정책과 프로세스 콘텐츠를 선택할 수 있는 유연성을 보장한다. 예를 들어, OpenChain 적합 프로그램은 단일 제품군 또는 전체 조직을 대상으로 적용할 수 있다.

이 소개에서는 모든 잠재적 사용자를 위한 개요를 제공한다. 2 장에서는 이 문서 전체에서 사용되는 주요 용어를 정의한다. 3 장에서는 프로그램이 OpenChain 에 적합하기 위해 충족해야 하는 요구 사항을 정의한다. 각 요구 사항은 이를 충족하기 위해 생성해야 하는 하나 이상의 입증 자료(문서 등)를 포함한다. 입증 자료를 공개해야 하는 것은 아니지만, 필요할 경우 NDA(Non-Disclosure Agreement)를 맺고 다른 조직에 제공할 수 있다.

이 문서는 200 명 이상의 기여자들로부터 피드백을 받아 오픈 이니셔티브로 개발되었다. 역사적인 발전 과정을 이해하기 위해서는 Specification Mailing List 와 FAQ 를 참고할 수 있다.

이 규격은 Creative Commons Attribution License 4.0 (CC-BY-4.0)에 따라 라이선스가 부여된다.

정보 기술– OpenChain 규격

1 적용 범위

이 문서는 오픈소스로 구성된 소프트웨어 솔루션을 주고 받는 조직 간에 신뢰를 구축하기 위한 기준을 제공하기 위해 우수한 오픈소스 라이선스 컴플라이언스 프로그램의 핵심 요구사항을 정의한다.

2 용어와 정의

이 문서의 목적을 위해 다음과 같은 용어와 정의를 적용한다.

2.1
컴플라이언스 산출물
컴플라이언스 프로그램의 결과물을 나타내며 배포용 소프트웨어와 함께 제공해야 하는 산출물의 모음이다.

참고: 여기에는 다음 사항이 포함된다(단, 이에 국한되지 않음) : 저작자 고지, 소스 코드, 빌드 및 설치 스크립트, 라이선스 사본, 저작권 고지, 수정 내용 고지, 서면 청약(Written Offer), 오픈소스 컴포넌트 BOM (Bill of Materials), SPDX 문서.

2.2
식별된 라이선스
배포용 소프트웨어에 포함된 오픈소스 컴포넌트를 식별하기 위한 적절한 방법으로 식별된 일련의 오픈소스 라이선스 집합이다.

2.3
OpenChain 적합(Conformant)
이 문서의 모든 요구사항을 충족하는 프로그램이다.

2.4
오픈소스
Open Source Initiative 에서 만든 Open Source Definition (opensource.org/osd) 혹은 Free Software Foundation 에서 만든 Free Software Definition (gnu.org/philosophy/free-sw.html)을 충족하는 라이선스, 혹은 이와 유사한 라이선스가 하나 이상 적용된 소프트웨어이다.

2.5
프로그램
조직의 오픈소스 라이선스 컴플라이언스 활동을 구성하는 정책, 프로세스 및 인력의 집합이다.

2.6
프로그램 참여자
배포용 소프트웨어를 만들고, 이에 기여하거나 준비할 책임이 있는 모든 조직 구성원 혹은 계약자이다.

© Joint Development Foundation 2020 –자세한 내용 및 자체 인증은 www.openchainproject.org 참조

참고: 조직에 따라 소프트웨어 개발자, 릴리스 엔지니어, 품질 엔지니어, 제품 마케팅 및 제품 관리자가 포함될 수 있다 (단, 이에 국한되지는 않는다).

2.7
SPDX
소프트웨어 패키지를 주고 받을 때 라이선스 및 저작권 정보를 포함한 BOM(Bill of Materials)을 교환하기 위해 Linux Fouindation 의 SPDX(Software Package Data Exchange) Working Group 에서 만든 형식 표준이다(spdx.org 참조).

2.8
배포용 소프트웨어
조직이 제 3 자(예: 다른 조직 또는 개인)에게 배포하는 소프트웨어이다.

2.9
입증 자료
규격의 요구사항이 충족되었음을 입증하는 자료이다.

ISO 및 IEC 는 다음 주소에서 표준화에 사용할 용어 데이터베이스를 유지한다:

- ISO Online browsing platform: https://www.iso.org/obp
- IEC Electropedia: http://www.electropedia.org/

3 요구사항

3.1 프로그램 설립

3.1.1 정책

배포용 소프트웨어의 오픈소스 라이선스 컴플라이언스를 관리하는 문서화된 오픈소스 정책이 있어야 한다. 이 정책은 조직 내부에 전파되어야 한다.

입증 자료:

- 3.1.1.1 문서화된 오픈소스 정책.
- 3.1.1.2 프로그램 참여자가 오픈소스 정책의 존재를 알 수 있게 하는 문서화 된 절차 (교육, 내부 위키, 혹은 기타 실질적인 전달 방법 등)

이유:

오픈소스 정책을 만들고, 프로그램 참여자가 오픈소스 정책의 존재를 인식하도록 보장하기 위해서이다. 정책에 어떤 사항이 포함되어야 하는 지에 대해서는 다음 섹션에서 다룬다

3.1.2 역량

조직은 다음 사항을 수행해야 한다

- 프로그램의 성과와 효율에 영향을 미치는 역할이 무엇인지, 그 역할에 해당하는 책임은 무엇인지 확인한다.

 © Joint Development Foundation 2020 –자세한 내용 및 자체 인증은 www.openchainproject.org 참조

- 각 역할을 수행할 프로그램 참여자가 갖춰야 할 필요 역량을 결정한다.
- 프로그램 참여자가 적절한 교육, 훈련 및/또는 경험을 바탕으로 자격을 갖춘 자임을 확인한다.
- 해당되는 경우, 필요한 역량을 확보하기 위해 조치한다.
- 역량 보유를 증명하기 위한 정보를 문서화하여 유지한다.

입증 자료:

- 3.1.2.1 프로그램의 여러 참여자에 대한 역할과 각 역할의 책임을 나열한 문서
- 3.1.2.2 각 역할을 위해 필요한 역량을 기술한 문서
- 3.1.2.3 각 프로그램 참여자의 역량을 평가한 문서화된 증거

이유:

프로그램 참여자가 각자의 역할과 책임을 위한 충분한 수준의 역량을 확보하였음을 보장하기 위해서이다.

3.1.3 인식

조직은 프로그램 참여자가 다음 사항을 인식하도록 보장해야 한다:

- 오픈소스 정책;
- 오픈소스 관련 목표;
- 효과적인 프로그램이 되기 위한 참여자의 기여 방법
- 프로그램 요구사항을 준수하지 않을 경우 미치는 영향

입증 자료:

- 3.1.3.1 다음 사항에 대한 프로그램 참여자의 인식을 평가하였음을 나타내는 문서화된 증거 : 프로그램의 목표, 프로그램 내에서의 참여자 기여 방법 및 프로그램을 준수하지 않을 경우 미치는 영향

이유:

프로그램 참여자가 프로그램 내에서 각자의 역할과 책임에 대해 충분한 수준의 인식을 갖고 있음을 보장하기 위해서이다.

3.1.4 프로그램 적용 범위

프로그램은 다양한 범위 별로 적용하여 관리할 수 있다. 예를 들어, 한 프로그램을 단일 제품군에만 적용할 수도 있고, 전체 부서 또는 전체 조직에 적용하여 관리할 수 있다. 따라서 각 프로그램에서는 적용 범위를 정확히 명시해야 한다.

입증 자료:

- 3.1.4.1 프로그램의 적용 범위와 한계를 명확하게 정의한 문서화된 진술

이유:

조직의 필요 범위에 맞게 가장 적합한 프로그램을 유연하게 구성하기 위해서이다. 어떤 조직은 프로그램을 특정 제품군을 관리하도록 적용할 수 있고, 또 어떤 프로그램은 전체 조직에서 배포하는 소프트웨어를 관리하도록 지정할 수 있다.

3.1.5 라이선스 의무

각 라이선스에 의해 부과된 의무, 제한 및 권리를 알아내기 위해 식별된 라이선스를 검토하는 프로세스가 있어야 한다.

입증 자료:

- 3.1.5.1 각 식별된 라이선스에 의해 부여된 의무, 제한 및 권리를 검토하고 기록하기 위한 문서화된 절차

이유:

조직이 직면할 수 있는 다양한 사용 사례(3.3.2 조 정의)에 대해 식별된 각 라이선스의 의무를 검토하고 확인하는 프로세스가 있음을 보장하기 위해서이다.

3.2 관련 업무 정의 및 지원

3.2.1 외부 문의 대응 (Access)

외부의 오픈소스 문의에 효과적으로 대응하기 위한 프로세스를 유지해야한다. 제 3 자가 오픈소스 컴플라이언스에 대해 문의 할 수 있는 방법을 공개해야 한다.

입증 자료:

- 3.2.1.1 제 3 자가 오픈소스 라이선스 컴플라이언스에 대해 문의 할 수 있는 공개된 방법 (담당자 이메일 주소, 또는 Linux Foundation 의 Open Compliance Directory 활용 등)
- 3.2.1.2 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 방법을 제공하고, 조직이 이를 효과적으로 대응할 수 있는 준비가 되어 있는지 보장하기 위해서이다.

3.2.2 효과적인 리소스 제공

프로그램이 효과적일 수 있도록 다음과 같이 업무를 정의하고 리소스를 제공해야 한다:

- 프로그램을 성공적으로 수행할 수 있도록 각 업무에 대한 책임을 할당한다.
- 프로그램의 업무를 위한 충분한 리소스를 제공한다.
  - 업무 수행 시간을 할당한다.
  - 예산을 적절하게 지원한다.
- 정책 및 지원 업무를 검토하고 개선하는 프로세스가 존재한다.
- 오픈소스 라이선스 컴플라이언스와 관련된 전문 법률 자문을 이용 할 수 있게 한다.

 © Joint Development Foundation 2020 –자세한 내용 및 자체 인증은 www.openchainproject.org 참조

- 오픈소스 라이선스 컴플라이언스 문제를 해결하기 위한 프로세스가 존재한다.

입증 자료:

- 3.2.2.1 프로그램 내 각 역할을 담당하는 인원, 그룹 또는 직무의 이름을 기재한 문서
- 3.2.2.2 프로그램 내 각 역할을 담당하는 인원이 적합하게 배치되고, 예산이 적절하게 지원되어야 한다.
- 3.2.2.3 오픈소스 라이선스 컴플라이언스 문제 해결을 위해 내부 또는 외부의 전문 법률 자문을 이용할 수 있는 방법
- 3.2.2.4 오픈소스 컴플라이언스에 대한 내부 책임을 할당하는 문서화된 절차
- 3.2.2.5 미준수 사례를 검토하고 이를 수정하기 위한 문서화된 절차

이유:

i) 프로그램 내 각 역할을 효과적으로 지원하며 리소스를 제공하고, ii) 정책 및 지원 프로세스가 오픈소스 컴플라이언스 모범 사례의 변경 사항을 수용하도록 정기적으로 업데이트되고 있음을 보장하기 위해서이다.

3.3 오픈소스 콘텐츠 검토 및 승인

3.3.1 BOM (Bill of Materials)

배포용 소프트웨어를 구성하는 오픈소스 컴포넌트(및 식별된 라이선스)에 대한 BOM(Bill of Materials)을 생성하고 관리하는 프로세스가 있어야 한다.

입증 자료:

- 3.3.1.1 배포용 소프트웨어를 구성하는 오픈소스 컴포넌트에 대한 정보를 식별, 추적, 검토, 승인 및 보관하는 문서화된 절차
- 3.3.1.2 문서화된 절차가 적절히 준수되었음을 보여주는 배포용 소프트웨어에 대한 오픈소스 컴포넌트 기록

이유:

배포용 소프트웨어를 구성하는데 사용되는 오픈소스 컴포넌트 BOM 을 생성하고 관리하기 위한 프로세스가 있음을 보장하기 위해서이다. 배포용 소프트웨어를 배포하는데 적용되는 의무와 제한 사항을 이해하기 위해서는 각 컴포넌트의 라이선스 조항에 대한 체계적인 검토 및 승인을 지원하는 BOM 이 필요하다.

3.3.2 라이선스 컴플라이언스

프로그램은 배포용 소프트웨어에 대해 프로그램 참여자가 접할 수 있는 일반적인 오픈소스 라이선스의 사용 사례를 관리할 수 있어야 한다. 여기에는 다음과 같은 사용 사례가 포함될 수 있다(아래 목록이 모든 사례를 다루는 것은 아니며, 또한 이 사례를 모두 다뤄야만 하는 것은 아님). :

- 바이너리 형태로 배포
- 소스 형태로 배포
- 추가 라이선스 의무를 유발하는 다른 오픈소스와 통합
- 수정된 오픈소스 포함

- 배포용 소프트웨어 내의 다른 컴포넌트와 서로 호환되지 않는 라이선스 하의 오픈소스 또는 다른 소프트웨어를 포함
- 저작자 표시 요구사항을 갖는 오픈소스 포함

입증 자료:

- 3.3.2.1 배포용 소프트웨어 내의 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 절차가 준수됨을 보장하기 위해서이다.

3.4 컴플라이언스 산출물 생성 및 전달

3.4.1 컴플라이언스 산출물

배포용 소프트웨어에 대한 컴플라이언스 산출물을 생성하는 프로세스가 있어야 한다.

입증 자료:

- 3.4.1.1 식별된 라이선스가 요구하는 컴플라이언스 산출물을 준비하고, 이를 배포용 소프트웨어와 함께 제공하기 위한 프로세스를 설명하는 문서화된 절차
- 3.4.1.2 배포용 소프트웨어의 컴플라이언스 산출물 사본을 보관하기 위한 문서화된 절차 - 산출물 사본은 배포용 소프트웨어의 마지막 배포 이후 합리적인 기간1 동안 혹은 식별된 라이선스에서 요구하는 기간 동안 보관해야 한다(둘 중 더 긴 기간을 따름). 이러한 절차가 올바르게 수행되었음을 입증하는 기록이 존재해야 한다.

이유:

식별된 라이선스에서 요구하는 대로 배포용 소프트웨어와 함께 제공해야 하는 컴플라이언스 산출물을 준비하는데 합당한 상업적 노력을 기울이고 있음을 보장하기 위해서이다.

3.5 오픈소스 커뮤니티 참여에 대한 이해

3.5.1 기여

조직이 외부 오픈소스 프로젝트로의 기여를 허용하려고 한다면,

- 오픈소스 프로젝트로의 기여를 관리하는 문서화된 정책이 있어야 한다.
- 이 정책을 내부에 전파해야 한다.
- 정책을 시행하는 프로세스가 있어야 한다.

[1] 도메인, 법적 관할권 또는 고객 계약에 따라 결정

 © Joint Development Foundation 2020 –자세한 내용 및 자체 인증은 www.openchainproject.org 참조

입증 자료:

조직이 외부 오픈소스 프로젝트로의 기여를 허용하는 경우, 다음 사항이 있어야 한다. :

- 3.5.1.1 문서화된 오픈소스 기여 정책
- 3.5.1.2 오픈소스 기여를 관리하는 문서화된 절차
- 3.5.1.3 모든 프로그램 참여자가 오픈소스 기여 정책의 존재를 인식하도록 하는 문서화된 절차 (예: 교육, 내부 위키, 또는 기타 실질적인 전달 방법 등)

이유:

조직이 오픈소스 기여를 허용하려 한다면, 먼저 기여 정책을 수립하고 이를 이행하는데 필요한 사항을 합리적으로 고려하게 하기 위해서이다. 오픈소스 기여 정책은 전체 오픈소스 정책의 일부로 포함시키거나, 자체적인 별도의 정책이 될 수도 있다.

3.6 규격 요구사항 준수

3.6.1 적합성 (Conformance)

프로그램이 OpenChain 에 적합하다고 간주하기 위해서는 조직은 프로그램이 이 규격에서 제시한 모든 요구사항을 충족하는지 확인해야 한다.

입증 자료:

- 3.6.1.1 3.1.4 조에서 명시한 프로그램이 이 규격의 모든 요구사항을 충족함을 확인하는 문서

이유:

조직이 OpenChain 에 적합한 프로그램을 보유했다고 선언하는 것은 그 프로그램이 이 문서의 모든 요구사항을 충족하고 있음을 보장하기 위해서이다. 이 요구사항의 일부 만을 충족하는 것으로는 충분하지 않다.

3.6.2 지속 기간

이 규격의 버전 2.1 에 적합한 OpenChain 프로그램은 적합성 인증을 획득한 날로부터 18 개월 동안 지속되어야 한다. 적합성 인증 등록 절차는 OpenChain 프로젝트의 웹사이트에서 확인할 수 있다.

입증 자료:

- 3.6.2.1 프로그램이 적합성 인증을 획득한 후 지난 18 개월 동안 이 규격 버전(v2.1)의 모든 요구사항을 충족하고 있음을 확인하는 문서

이유:

조직이 시간이 지나도 적합성을 주장하고자 한다면 프로그램을 규격에 맞게 계속 유지하는 것이 중요하다. 이 요구사항은 시간이 지난 후 조직이 계속해서 프로그램 적합성을 주장하더라도 프로그램의 지원 프로세스와 통제가 약화되지 않았음을 보장하기 위해서이다.

부록 A

(정보)

다국어 번역

글로벌 채택을 촉진하기 위해 규격을 다른 언어로 번역하려는 노력을 매우 환영한다. OpenChain 은 오픈소스 프로젝트로서 동작하기 때문에 다국어 번역은 번역 작업에 시간과 전문지식을 기꺼이 기여한 사람들에 의해 이루어진다. 번역은 i) CC-BY-4.0 라이선스의 조건에 따라 제공되며 ii) 프로젝트의 번역 정책 정책을 따른다. 정책에 대한 세부 정보와 공개된 번역은 OpenChain 프로젝트의 wiki 에서 확인할 수 있다.

© Joint Development Foundation 2020 –자세한 내용 및 자체 인증은 www.openchainproject.org 참조