

OSS 거버넌스 동향과 라이선스 분석 툴

박정현 박영식* 김현기* 김영길**

한국전자통신연구원 책임연구원

한국전자통신연구원 실장 *

한국전자통신연구원 그룹장 **

I. 서론

기술 및 제품 개발 시간 단축과 비용 절감, 기술 종속성 탈피, 그 외 자유롭게 사용할 수 있는 권리와 절약된 노력으로 기술과 제품 개발 수준 향상 등 OSS(Open Source Software) 활용 목적은 분명하기에 OSS 활용은 계속 증가할 것으로 기대된다. 실제 현재 70% 이상의 기업에서 기술과 제품을 개발하는데 OSS를 활용하고 있는 것으로 조사되고 있으며[3], 앞으로 4차 산업 혁명 시대를 맞이하면서 IoT, AI, 빅데이터, 클라우드 컴퓨팅, 차세대 모바일 기술 등 신 기술 분야에서 오픈소스 활용은 더욱 확대될 것으로 보인다. 이렇듯 빠른 기술 변화와 소프트웨어 패러다임 변화 속에서 ICBM(사물인터넷, 클라우드, 빅데이터, 모바일)을 활용한 산업 혁신이 필요한 상황에 직면한 기업에서의 OSS 활용 증대는 더욱 가속화될 것으로 기대된다. 정부 및 공공기관에서도 정보화 사업 수행에 있어 활용되는 OSS 규정 및 지침을 제시하고, 정보화사업 단계별 관리·점검 가이드 3.0을 기반으로 공개 소프트웨어의 관리요소 및 고려사항을 보완한 거버넌스 가이드를 제시하고 있다[6]-[8]. ICT 분야에서 다양한 R&D 과제를 수행하는 ETRI에서도 SW 개발이나 아웃소싱을 통한 기술 개발에서 오픈 소스 사용 비중은 점점 늘어나고 있는 실정이다. 이에 본 고에서는 새로운 기술과 제품 개발에서 OSS 활용 증대에 따라 조직에서 더욱 요구되는 OSS 거버넌스와 라이선스 분석 및 검증 툴을 조사하였다. 본 고에서는 I장에서는 OSS 거버넌스 필요성, II장에서는 국내외 기업의 OSS 거버넌스 동향, III장에서는 OSS 라이선스 분석 및 검증을 위해 사용 가능한 툴 동향, IV장에서 전체 내용을 요약한다.

* 본 내용은 박정현 책임연구원(042-860-5512 jh-park@etri.re.kr)에게 문의하시기 바랍니다.

** 본 내용은 필자의 주관적인 의견이며 ITP의 공식적인 입장이 아님을 밝힙니다.

II. OSS 거버넌스 동향

1. 국내

가. KT DS

KT DS는 2006년부터 오픈소스 도입에 대한 검토를 진행해서 2010년 11월에 오픈소스 마스터 플랜을 수립하였고, 2011년 Pilot 시범 운영을 통해 표준을 준비한 후, 2013년부터 Roadmap 준비를 통해 현재까지 오픈소스 도입 확산을 진행해 오고 있다. KT DS의 오픈소스 도입 체계는 기업의 비용 절감 측면에서 전략적으로 탑 다운(Top-Down) 형태를 띠고 있으나 기본적으로 비즈니스 영역 증대가 고려되고 가치제공 측면, 자원관리 측면, 위험관리 측면, 성과 측면, 전략적 연계 측면이 고려된 거버넌스 체계를 갖추고 있다. KT DS는 오픈소스 도입을 위한 프로세스와 조직 그리고 툴을 이미 구축하여 진행해오고 있으며, 오픈소스 조사, 평가, PoC(Proof of Concept), Pilot, 도입 의사 결정, 전사 적용, 기술 지원, 업그레이드 및 폐기 등 8 단계의 오픈소스 도입 라이프 사이클을 운영해 오고 있다. 이 외 KT DS는 오픈소스 관련 조직 운영을 통해 거버넌스 기능, 개발/운영 기능, 기술지원 기능, 관련 기술 교육 등 서비스 기능, 오픈소스 제품 품질 보증 지원 기능 등을 커버하고 있다.

나. LG 전자

LG 전자는 OSS 거버넌스를 위해 공개 SW 라이선스 컴플라이언스라는 이름으로 OSS를 위한 조직 구성, 프로세스 및 정책 수립, 그리고 툴을 구축하여 운영해 오고 있다. 조직으로는 전사적으로 오픈소스 컴플라이언스 팀을 구성하고 팀의 총괄 지원 아래 사업부별 오픈소스 컴플라이언스 담당자가 있다. 전사적 팀에서는 현재 6명이 컴플라이언스 전략을 수립하고, 정책과 프로세스를 구축 및 제공하며, 효율화를 위한 자동화 도구 제공, 교육, 외부 대응 등을 수행하고 있다. 또한, LG 전자의 공개 SW 라이선스 컴플라이언스 활동내용으로는 국내외 개발자 대상의 주기적인 공개 SW 라이선스 교육, 온라인 교육, 분기별 각 사업부 담당자 대상의 Open Source Compliance Workshop 개최, 매월 세미나 형태의 Open Source License Forum 개최, 공개 SW 관련 동향 및 사내 이슈에 대한 newsletter 격월 발행, 전 사업부에서 공개 SW를 사용하면서 준수해야 할 사항에 대한 정보 제공 등을 수행하고 있다.

다. CJ

CJ는 OSS 거버넌스 구축을 통해 오픈소스 도입부터 운용에 이르기까지 종합관리체계를 갖추고 있으며 오픈소스 정책 및 절차 관리, 표준기술 적용 및 신규 버전 검증, 소스코드 검증을 통한 라이선스 관리, 보안취약점 점검 및 예방, 정보검색 및 제공 등을 수행하고 있다. CJ는 OSS 거버넌스 포털 구축 및 운영을 통해 프로젝트 및 서비스별 OSS 등록 및 승인 등 OSS 사용과 검증에 대해 체계적인 관리를 하고 있으며, 글로벌 오픈소스 목록 검색 및 검토시 환경 및 보안 등의 문제를 검증하고, 포털 게시판을 통해 커뮤니티 활동 내용과 공지사항, OSS 가이드 등을 제공하며, 오픈소스 모니터링 기능을 통해 오픈소스 사용·검증·승인에 대한 통계 그래프 도식화, 라이선스 및 보안 현황 모니터링, 오픈소스 코드 분석을 통해 검증보고서 리포트 산출 기능 등을 지원하고 있다. 또한, 오픈소스 프로세스를 수립하여 운영하고 있는데, 그 프로세스는 솔루션과 플랫폼 도입 시 서비스 및 기능 대체 신규도입 솔루션 검토 요구 단계, 필요기능 및 IT 환경 조사 및 비즈니스 영향에 대한 검토 단계, 후보 오픈소스의 발굴 및 대체 소프트웨어 선정 단계, 오픈소스의 기본기능 강화 및 추가 개발 단계, 그리고 오픈소스 솔루션 단독 설치 또는 클라우드 서비스로의 제품화 단계 과정으로 구성되어 있다. 이 외 CJ는 오픈소스 기술 지원 활동으로 오픈소스 전문조직 및 인력을 운영하고 있으며, 오픈소스 기술 지원 채널 구축, 오픈 SW 컨설팅, 상용 SW의 오픈 SW로의 전환 지원, 그리고 오픈 소스 설치 및 유지보수 업무 등을 수행하고 있다.

라. SK텔레콤

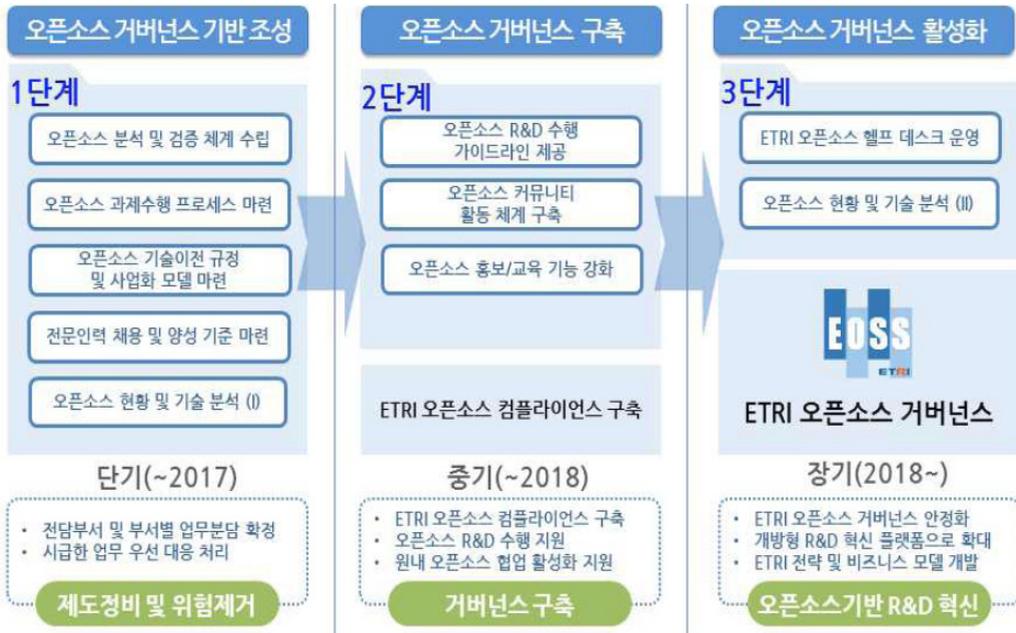
SK텔레콤은 OSS 컴플라이언스를 위해 OSS 거버넌스 조직 구성과 프로세스 수립, 그리고 OSS 라이선스 검증을 위한 환경을 구축하여 운영해 오고 있다. SK텔레콤의 OSS 컴플라이언스를 위한 내부 조직은 OSS 거버넌스를 총괄하고 OSS 정책과 전략을 수립하며, OSS 정책 위반 사항을 확인하고 오픈소스 고지문 작성 지원과 동시에 오픈소스에 대한 외부 문제와 상황에 따른 대응 업무를 수행하는 IPR팀, OSS 검증 대상을 선정하고, OSS 사용 계획을 검토하며 라이선스 검증을 확인하는 IT혁신팀, 그리고 OSS 검증을 신청하고, OSS 사용 계획을 수립하며, OSS 검증 결과를 통해 위반 사항에 대해 조치한 후 소스코드를 등록하고 고지문을 포함하여 소스를 배포하는 개발팀 형태로 구성 및 운영되고 있다. SK텔레콤은 OSS 거버넌스를 위해 내부 시스템을 구축하여 운영하고 있으며 동시에 내부 기술 지원 그룹 결성과 구성원 교육을 수행하고 있다. 이 외 지속적인 변화 관리와 환경 변화에 대한 대응, 비즈니스 파트너까지의 OSS 검증 지원을 수행하며 리거시 프로세스 및 시스템과의 연동까지 고려하여 업무를 수행하고 있다.

마. 삼성전자

삼성전자는 OSS 거버넌스를 위해 OSAB(Open Source Advisory Board)를 구성 및 운영해 오고 있으며, OSAB에서는 OSS 정책 수립과 감사를 위한 조직, 오픈소스 도입 및 검토를 위한 조직, 라이선스 검증과 기술 지원을 위한 조직, 그리고 외부 문제 대응을 위한 조직 형태로 운영하고 있다. 삼성전자는 각각의 프로젝트에서 오픈소스를 사용해 개발한 SW를 포함하여 제3자를 통해 개발한 SW, 상용 SW, 그리고 자체 개발한 SW 등 모든 SW에 대해 오픈소스 사용 여부에 대한 식별부터 라이선스 분석 및 검증에 이르기까지 10 단계 과정을 통해 진행하고 있다. OSS 분석과 검증 단계에서는 소스코드 스캔 방식을 통해 검증하고 있으며 동시에 Checksum을 통해 추가적인 확인을 진행한다. 또한 검증 완료된 개발 소스와 오픈소스에 대해서는 AIRS(Auto IdentifieR using SPDX: Software Package Data Exchange)를 통해 고지문을 준비하여 공개 및 배포하고 있으며 오픈소스에 대한 공개 및 고지 의무사항 준수를 위해 OSRC(Open Source Release Center)를 구축하여 운영하고 있다. 이 외 삼성전자는 오픈소스 커뮤니티 기여 활동에 참여하는 프로세스를 수립하여 운영하고 있으며 실제 삼성전자는 매년 삼성 오픈소스 컨퍼런스(Samsung Open Source CONference: SOSCON)를 개최하고 있고 삼성개발자 회의(Samsung Developer Conference: SDC)와 Tizen 개발자 회의(Tizen Developer Conference: TDC)를 개최 및 운영하고 있다.

바. ETRI

ETRI는 OSS 거버넌스 구축을 위해 2017년 이전에는 기반 조성 단계를 준비하였고, 2017년부터는 오픈소스센터 조직 구성 및 운영을 통해 오픈소스 정책 및 전략 수립, 라이선스 특허 분쟁 지원, 라이선스 검사 지원, 교육 및 홍보, 커뮤니티 지원 등의 활동을 해오고 있다. 또한, 2018년부터는 OSS 거버넌스 활성화를 통해 오픈소스 현황 및 기술 분석 활동과 동시에 ETRI 오픈소스 헬프 데스크 운영을 준비하고 있다. 이 외 ETRI는 오픈소스 라이선스 검증을 위한 프로세스를 수립하여 운영하고 있으며 오픈소스 라이선스 검증 환경 구축을 통해 각각의 프로젝트에서 개발한 모든 기술 이전 대상 개발 SW에 대해서는 사전에 반드시 OSS 라이선스 검증을 완료 후, 개발된 SW가 외부 이전할 수 있도록 하고 있다. [그림 1]은 현재 ETRI에서 OSS 거버넌스를 위해 진행하는 전략 및 과정이다.



(자료) ETRI, 오픈소스 SW 대응 추진 계획, 2017. 5.

[그림 1] ETRI OSS 거버넌스 대응

2. 국외[5]-[7]

가. 레드햇

레드햇은 1993년 설립되어 오픈 SW 에코 시스템을 기반으로 클라우드 컴퓨팅, 미들웨어, 가상화 및 모바일 등 다양한 분야에서 오픈 협업 비즈니스 모델과 서브스크립션 모델을 사용하여 연매출 20억 달러 이상의 성공을 거듭하고 있다. 이 외 레드햇은 오픈 SW 분야에 대한 신뢰성을 보증하는 서브스크립션 모델과 교육을 통해 오픈 SW 생태계에 참여하고 있으며, 오픈 SW 커뮤니티에 대한 지원을 지속적으로 하고 있다.

나. 마이크로소프트

마이크로소프트는 세계 최대의 소프트웨어 및 하드웨어 개발·판매 업체이며 가장 유명한 제품으로는 MS 윈도 운영체제가 있다. 전통적인 비공개 SW를 판매하는 대표적인 기업이던 마이크로소프트 역시 다른 기업들과 마찬가지로 기존의 비즈니스 전략에서 오픈 SW를 활용한 전략으로 변경하고 있다. 마이크로소프트는 직원들의 오픈 SW 활동을 독려하며 오픈 SW 생태계에 적극적인 러브

콜을 보내고 있다. 2009년 OSCON(Open Source Conference)에서 2만 줄의 리눅스 드라이버 소스 코드를 공개하고 아파치 재단에 10만 달러를 기부하는 등 활발한 오픈 SW 커뮤니티 협력 활동도 펼치고 있다. 특히, 2015년에는 대표적인 오픈 SW 기업인 레드햇과 파트너십을 체결하여 클라우드 시장에서의 협업을 통한 비즈니스 활성화를 모색하고 있으며, 주요 솔루션의 소스 코드를 공개하는 등 오픈 SW를 품안에 끌어안는 정책을 펼치고 있다.

다. 오라클

오라클은 Linux, PHP, Apache, Eclipse, Berkeley DB 및 InnoDB 등 오픈 SW 기술을 개발하고 테스트 및 최적화하고 지원하는데 막대한 자원을 투자하고 있으며, 오픈 SW 솔루션 제품을 개발하여 배포하는 활동을 지원하고 있고 오픈 SW가 포함된 제품으로 비즈니스를 하고 있다. 이외 오라클은 미션 크리티컬 환경에서 저비용, 관리 가능성 향상, 가용성 증대 및 신뢰성, 성능, 확장성 증가 등의 이유로 오픈 SW 기술을 함께 사용하고 있다.

라. IBM

메인 프레임용 시장과 PC 하드웨어에 이르기까지 컴퓨터와 관련된 모든 시장에서 승승장구하던 IBM이 마이크로소프트가 등장하면서 운영체제 시장에서 어려움을 겪었지만 자사의 웹스피어 제품군에 오픈 SW 프로젝트 아파치를 도입하며 다시 순항을 시작했다. IBM은 오픈 SW 아파치 프로젝트의 성공을 발판으로 2000년부터는 서비스 산업에 포커스를 맞추어 컨설팅, 소프트웨어 및 서비스 비즈니스의 매출 비중을 향상시키며 통합 솔루션 회사로 변신하였고 최근 빅데이터 분석 기술인 아파치 스파크를 10년간 지원하기로 결정하였다. 이외 IBM은 자사의 분석 플랫폼에 스파크를 통합하고 블루믹스 서비스 플랫폼으로 스파크를 제공하는 프로젝트에 3,500여명의 연구원과 개발자를 투입하고 향후 오픈 SW 기술인 스파크를 중심으로 빅데이터 분석 시장에 활용할 예정이다.

마. 구글

구글은 매일 10억 건 이상의 검색을 처리하는 세계 최대 인터넷 검색 서비스 회사로 오픈 SW 커뮤니티, 오픈 스택, 아파치 재단 등의 플래티넘 후원사로 활동하며 매년 큰 비용의 후원금을 지원하는 회사이다. 현재 세계에서 가장 많이 사용되는 모바일 운영체제 안드로이드를 2005년 569억에 인수하여 오픈 SW로 제공했다. 구글은 안드로이드 외에도 사용할 수 있는 글꼴, 웹 브라우저 크롬, 로열티 없는 고화질 영상 압축 포맷 WebM, 인공 지능 엔진 Tensor Flow를 공개하는 등 오픈 SW 생태계의 활성화를 위해 노력하는 대표적 기업이다.

III. OSS 라이선스와 분석 틀

1. OSS 라이선스

OSS는 말 그대로 공개된 SW로 누구나 언제든지 사용할 수 있는 SW이다. 다만, 공개된 SW를 사용 혹은 수정하여 제3자에게 배포하는 경우 혹은 공개된 SW를 사용 혹은 수정하여 기술이나 제품을 만들어 배포하는 경우에 OSS를 사용 및 수정한 SW 코드에 대해서는 사용 OSS 라이선스를 따르게 되며 일부 특정 OSS 라이선스의 경우에는 OSS 연관해서 개발한 기술 및 제품 전체 SW 소스 코드까지 공개 의무 사항을 갖는다. OSS 라이선스란, OSS는 SW로서 저작권자만이 해당 SW에 대한 사용 권리를 갖도록 지적재산권에 의해 보호를 받는데, 이런 해당 SW의 독점 사용 권리에 대해 SW 개발자와 사용자 간의 이용 방법과 조건을 명시한 대여 규칙을 정해 놓은 허가권을 의미한다. 따라서 OSS 라이선스는 공개 SW에 대한 이용 방법과 조건을 명시한 대여 규칙을 정해 놓은 허가권을 의미한다.

OSS 라이선스는 소스 코드의 공개 여부에 따라 강력한 상호 허가권(Strong Reciprocal License)

[표 1] 주요 OSS 라이선스 의무사항 비교[1]-[5]

주요 OSS 라이선스 의무사항	강력한 상호 허가권 (Strong Reciprocal License)			약한 상호 허가권 (Weak Reciprocal License)				관대한 허가권 (Permissive License)		
	GPL2	GPL3	AGPL3	LGPL2	LGPL3	MPL1	EPL1	MIT License	BSD3	Apache 2
1. 오픈소스의 자유로운 사용, 수정, 복사, 배포 가능 여부	0	0	0	0	0	0	0	0	0	0
2. 오픈소스 사용 후 사용 및 수정한 오픈소스 및 관련된 개발 SW 소스 코드의 제3자 배포 시(기술/제품/서비스 및 기술 이전 등) 수정한 오픈소스 내용 포함 개발한 SW 소스 코드의 공개 여부	사용 및 수정된 GPL 소스 코드와 링크 [정적/동적] 시 관련 모든 소스 코드 [사용, 수정, 링크된 소스 코드]를 GPL에 공개 의무 발생	사용 및 수정된 GPL 소스 코드와 링크 [정적/동적] 시 관련 모든 소스 코드 [사용, 수정, 링크된 소스 코드]를 GPL에 공개 의무 발생	사용 및 수정된 AGPL 소스 코드와 링크 [정적/동적] 시 관련 모든 소스 코드를 AGPL에 모두 공개 의무 발생	사용 및 수정된 LGPL 소스 코드와 정적 링크 시 관련 모든 오브젝트 코드 [사용, 수정, 링크된 소스 코드]를 LGPL에 공개 의무 발생	사용 및 수정된 LGPL 소스 코드와 정적 링크 시 관련 모든 오브젝트 코드 [사용, 수정, 링크된 소스 코드]를 LGPL에 공개 의무 발생	수정 및 추가된 MPL 코드가 포함된 파생 소스 코드를 GPL에 공개 의무 발생	수정 및 추가된 EPL 코드가 포함된 모순 소스 코드를 GPL에 공개 의무 발생	어떤 경우에도 공개 의무 없음	어떤 경우에도 공개 의무 없음	어떤 경우에도 소스 코드 공개 의무 없음
3. 오픈소스 사용 후 사용 및 수정한 오픈소스 및 관련된 개발 SW 소스 코드의 제 3자 배포 시 사용한 오픈 소스 수정 사항 및 관련된 개발 SW 소스 코드에 대한 라이선스 [영문] 고지 여부	0	0	0	0	0	0	0	0	0	0
4. 오픈소스 사용 후 변경한 오픈소스 및 개발 SW 소스 코드에 특이 사항이 포함되어 제 3자 배포 시 해당 특이 사항에 대해 무료 사용, 판매, 전송 행위 허락 여부 [특히 실시 허락 여부]	x	0	0	x	0	0	0	x	x	0
5. 오픈소스 사용 후 변경한 오픈소스 및 개발 SW 소스 코드에 특이 사항이 포함되어 제 3자 배포 시 해당 특이 사항/실시에 소송 제기 시 라이선스 종료 여부 [특히 보복 조항 유무]	x	0	0	x	0	0	0	x	x	0
6. 오픈소스 사용 및 복제에 따른 로열티 및 수수료 금지 여부	0	0	0	0	0	0	0	x	x	x
7. 오픈소스 사용 후 사용 및 수정 오픈소스 및 관련된 개발 SW 소스 코드의 제 3자 배포 시 사용 오픈 소스 수정 사항과 관련된 개발한 SW 소스 코드 이름, 상표, 상호 사용 금지 여부	x	x	x	x	x	0	x	x	x	x
8. 오픈소스 사용 및 복제에 따른 해당 오픈소스 최초 저자 보증 및 책임 여부	x	x	x	x	x	x	x	x	x	x

*GPL2/GPL3 (GNU General Public License version 2.0/3.0)
 *LGPL2/LGPL3 (GNU Library or Lesser General Public License version 2.0/3.0)
 *AGPL3 (Affero General Public License version 3.0)
 *MPL1 (Mozilla Public License version 1.0)
 *EPL1 (Eclipse Public License version 1.0)
 *BSD2 (BSD version 2.0)
 *Apache2 (Apache version 2.0)

을 갖는 것과 약한 상호 허가권(Weak Reciprocal License)을 갖는 것, 관대한 허가권(Permissive License)을 갖는 것으로 나눌 수 있다. 강력한 상호 허가권을 갖는 OSS 라이선스는 공개 SW의 일부 혹은 전체를 사용하여 SW를 개발한 경우에, 사용 혹은 수정한 공개 SW와 더불어 연관된 개발 SW 소스 코드 전체를 공개해야 하는 것으로, 대표적으로 AGPL-3.0, GPL-2.0, GPL-3.0 등이 있다. 그리고 약한 상호 허가권을 갖는 OSS 라이선스는 공개 SW의 일부 혹은 전체를 사용하여 SW를 개발한 경우에, 사용 혹은 수정한 공개 SW 소스 코드와 연관된 개발 SW 소스 코드 혹은 오브젝트 코드 일부를 공개하는 것으로, 대표적으로 MPL-2.0, LGPL-2.1 등이 있다. 마지막으로 관대한 허가권을 갖는 OSS 라이선스는 공개 SW의 일부 혹은 전체를 사용하여 SW를 개발한 경우에, 사용 혹은 수정한 공개 SW 소스 코드와 연관된 개발 SW 소스 코드를 공개하지 않아도 되는 것으로, 대표적으로 MIT, BSD 3-Clause, Apache-2.0 등이 있다. [표 1]은 주요 OSS에 대한 라이선스 의무 사항을 비교 및 요약한 것이다.

공개된 OSS는 누구든지 자유롭게 사용, 수정, 복제가 가능하다. 다만, OSS를 사용하여 기술 및 제품을 개발하여 3자에게 배포하거나 기술 이전을 하는 경우 수정 OSS 및 개발된 자체 SW 소스코드를 공개해야 하는 OSS 라이선스가 있음을 주의해야 하며, 이와 같은 라이선스를 갖는 대표적인 OSS가 GPL 계열과 AGPL 그리고 LGPL과 MPL 및 EPL 등으로 [표 1]에 정리하였다. 따라서 이런 계열의 OSS는 사용 후 기술이나 제품으로 만들거나 기술 이전을 통해 외부로 배포할 경우에 사용을 고려해야 할 것이다. 그리고 OSS를 사용하여 개발한 기술이나 제품의 SW 소스코드에 특허가 포함되어 있다면 공개된 SW 코드에서의 특허 권리 주장이 쉽지 않다는 사실도 OSS 사용 전에 미리 고려해야 하는 부분이다. 이 외 대부분의 OSS는 사용 후 OSS 수정 사항과 관련 라이선스를 고지해야 하는 의무가 있다는 사실도 기억할 필요가 있다.

2. OSS 라이선스 분석 툴[1],[2],[5]

OSS를 사용할 때는 반드시 사용할 OSS 라이선스를 사전에 확인할 필요가 있다. 사용한 OSS 라이선스 내용에 3자 배포에 따른 공개 의무가 있는 경우 OSS를 사용하여 만든 기술이나 제품 그리고 서비스와 연관된 관련 SW 소스코드를 모두 공개해야 하기 때문이다. 또한, 제품이나 기술 개발 일정이 촉박하여 OSS 라이선스의 사전 확인 없이 OSS를 사용하는 경우에는 개발된 기술이나 제품을 배포하기에 앞서 기술 개발에 사용한 OSS에 대한 라이선스 검증 과정이 필요하다. OSS 라이선스 검증은 개발 SW 소스코드의 크기에 따라 개발자가 스스로 확인하는 방법과 OSS 라이선스 검증 툴을 이용하여 자동으로 검증하는 방법이 있다.

사람에 의한 OSS 라이선스 검증이란 OSS를 이용하여 SW(소스 코드)를 개발하는 경우 먼저 사용한 혹은 사용하려는 해당 OSS 라이선스의 확인을 개발자 혹은 사용자 스스로 하는 것을 의미한다. 라이선스 확인을 통해 해당 라이선스의 의무 사항의 유지가 가능할 때 개발자 혹은 사용자는 OSS 사용 여부를 결정하고 해당 OSS를 사용하면 된다. 이때 해당 OSS의 라이선스 내용에 대한 해석을 개발자 혹은 사용자 혼자 판단하기 어려운 경우에는 법무팀의 협조를 받아 진행할 수 있다. 또한, 인터넷(구글 등) 소스코드 검색을 통해 찾아 사용하는 OSS의 경우에는 사용에 앞서 개발자 및 사용자는 해당 소스코드에 대한 최초 라이선스 확인이 필요하다. 이런 방법을 사람에 의해 수동으로 수행하는 OSS 라이선스 검증 방식이라 한다. 이렇게 개발자 혹은 사용자에 의해 OSS 라이선스를 사전에 확인하여 사용한 OSS와 관련하여 개발한 SW의 소스코드에 대해서는 개발 완료 후 추가적으로 OSS 라이선스 검증을 진행하지 않아도 된다. 따라서 OSS는 사용에 앞서 개발자 혹은 사용자가 사전에 라이선스 확인을 통해 OSS 사용 결정을 하는 것이 OSS 라이선스 검증을 위한 가장 좋은 방법이 될 수 있다.

한편, 툴을 이용한 OSS 라이선스 자동 검증이란 개발자 및 사용자가 OSS를 사용하여 SW를 개발한 경우에 개발한 소스코드에 대한 라이선스 검증을 자동화 툴을 이용하여 검증하는 방법을 의미한다. 툴을 이용한 OSS 라이선스 검증은 해당 소스코드를 스캔한 후 툴의 DB에 저장된 소스코드와 비교하여 검증하는 방식, 해당 소스코드 내 라이선스 혹은 주석문 문자열 검색 및 비교를 통해 OSS 라이선스를 검증하는 방식, 그리고 해당소스 코드에 대한 파일사이즈를 비교하여 Checksum 방식에 의한 파일 크기 비교를 통해 검증하는 방식 등이 있다.

이 외 툴과 사람에 의한 2중 검증 방식이 있으며, 이는 1차 툴을 이용하여 소스 코드 비교를 통해 확인하고, 확인된 OSS 중 2개 이상의 일치된 OSS에 대해 사람이 2차 검증하는 방식을 의미한다. OSS를 사용하여 개발한 소스코드 크기가 크고 OSS 라이선스 검증을 위한 시간적 여유가 없는 경우 툴을 이용하여 OSS 라이선스를 검증하는 것이 쉽고 빠를 수 있으나, 툴에 의한 방식은 기본적으로 소스코드의 유사 및 일치 패턴만을 찾아 줄 뿐이다. 이 경우 툴에서 찾아낸 유사 및 일치 패턴의 OSS 소스코드는 한 개 이상 검출될 수 있다. 이렇게 여러 개의 유사 및 일치 패턴 소스코드를 찾아 낸 경우 SW 개발에서 실제 사용한 OSS가 어떤 것인지 판단하기가 쉽지 않다. 더구나 오픈소스 특성상 시간이 지나면서 여러 개발자에 의해 수정 및 공개가 반복되면서 다수의 새로운 오픈소스로 배포될 수 있으며, 이런 경우 툴에서 찾아낸 여러 개의 OSS 중 실제 개발 SW에서 사용한 OSS를 찾아 그 라이선스를 확인하고 판단하는 것이 쉽지 않다. 따라서 1차 툴에서 찾아낸 OSS 중에서 실제 SW 개발에서 사용한 OSS를 판단하는 최종 결정은 사람(개발자/사용자)이 해야 한다. 이렇게 1차 툴에서 유사 및 일치한 소스코드를 찾아내고 찾아낸 여러 개의 OSS 중에서

실제 사용한 OSS를 사람이 최종 결정하므로 OSS 라이선스에 대한 정확한 검증이 진행될 수 있으며 이와 같은 검증 방식을 통과 사람에게 의한 2중 검증 방식이라 한다.

또한, 개발자 혹은 사용자는 OSS 소스코드 내 주석 정보나 고지 정보, 혹은 README 및 LICENSE 파일 내용의 추가적인 확인을 통해 SW 개발에서 실제 사용한 OSS와 그 라이선스에 대한 확인과 판단을 할 수 있다. 한편, OSS 라이선스 내용과 해석에 익숙하지 않은 개발자나 사용자는 SW 개발 과정에서 실제 사용한 OSS와 그 라이선스에 대한 정확한 판단을 하기가 쉽지가 않을 수 있으며, 또 OSS를 사용해 개발한 SW를 개발자가 아닌 다른 사람에게 의해 OSS 라이선스 검증을 진행하는 경우에는 OSS 라이선스 검증에 대한 잘못된 판단을 할 수도 있다. 따라서 OSS 라이선스 검증 툴을 이용하여 라이선스 검증을 진행한 경우에도 가능한 실제 OSS를 사용해 개발한 SW 개발자가 직접 OSS 라이선스 검증을 진행하는 것이 바람직하며, OSS 라이선스 내용에 대한 해석은 법률적 도움을 통해 진행하는 것이 바람직하다. 무엇보다도 SW 개발 과정에서 개발자는 가능한 OSS 사용 전 해당 OSS 라이선스를 미리 확인하고 사용하는 것이 가장 바람직한 방법이 될 수 있다.

[표 2]는 OSS 라이선스 검증을 위해 현재 사용 가능한 상용 OSS 라이선스 분석 툴을 정리한 것이다. 국내에서는 OSS 라이선스 자동 검증 툴로 Protex를 가장 많이 사용하는 편이다. ETRI를

[표 2] OSS 분석 자동화 도구 1 (상용)

도구명	제조사/라이선스	분석 방법	특징	비고
Protex	Black Duck→Synopsys (BDSK*)	소스 코드 비교 분석/ 바이너리(기능) 비교 분석	Code/Binary Scanning	https://www.blackducksoftware.com/ ; https://www.synopsys.com/ [ETRI, NIPA**, 국방기술품질원, LG, 삼성, KT, 네이버 등 사용 중]
code Eye	한국저작권위원회	소스 코드 비교 분석	Code Scanning	https://www.olis.or.kr/ ; [무료 검증 서비스 지원]
Protecode	Synopsys	소스 코드 비교 분석	Code Scanning	https://www.protecode.com/
WhiteSource	WhiteSource	소스 코드 비교 분석	Code Scanning	https://www.whitesourcesoftware.com/
Palarnida	FlexNet Code Insight	소스 코드 비교 분석	Code Scanning	https://www.palamida.com/
FOSSID	FOSSID	소스 코드 비교 분석	Code Scanning	https://fossid.com/
OpenLogic	RogueWave	소스 코드 비교 분석	Code Scanning	https://www.roquewave.com/
BAT	Apache-2.0→Synopsys	바이너리 분석	Binary Scanning	https://www.binaryanalysis.org/
Codonomicon AppCheck	Synopsys	바이너리 분석	Binary Scanning	https://www.codonomicon.com/ ; https://www.synopsys.com/

* BDSK: Black Duck Software Korea

** NIPA[공개SW 역량 프라자], <https://www.oss.kr/>:[무료 검증 서비스 지원]

포함하여 NIPA, LG, KT, 그리고 CJ 등에서 OSS 라이선스 자동 검증 툴로 사용하고 있는 Protex는 Black Duck 회사가 개발하여 판매 및 서비스해 왔으며, 지금은 Synopsys사에 인수되어 판매 및 서비스가 이루어지고 있다. 또한, 대부분의 OSS 라이선스 자동 검증 툴은 소스 코드를 스캔하여 툴 서버 DB에 갖고 있는 OSS 코드와 비교를 통해 라이선스를 검증하는 방식을 채택하고 있으며, 이 외 바이너리 및 실행 파일을 분석하는 툴도 일부 있다. 한국저작권위원회에서는 오픈소스 기반 OSS 라이선스 검증 툴인 Code Eye를 개발해 OSS 검증 및 컨설팅 서비스를 무료로 지원하고 있으며, NIPA도 공개 SW 역량 프라자를 통해 OSS 라이선스 검증과 컨설팅 서비스를 무료로 지원하고 있다.

[표 3]은 OSS 라이선스 검증을 위해 사용 가능한 오픈소스 기반 OSS 라이선스 분석 툴이다.

오픈소스 기반 OSS 라이선스 자동 검증 툴은 FOSSology가 대표적이며, 검증 방식은 소스코드 파일 내 라이선스 고지 문구 혹은 주석문 문자열 검색 및 비교를 통해 라이선스를 분석하는 툴이 대부분이다.

[표 3] OSS 분석 자동화 도구 II(오픈소스)

도구명	제조사/라이선스	분석 방법	특징	비고
FOSSology	GPL-2.0	소스코드 파일 내 라이선스 고지 문구(문자열)/주석문 분석	문자열 [탐색] 분석 도구	https://www.fossilology.org/
ScanCode & AboutCode	Apache-2.0	소스코드 파일 내 라이선스 고지 문구(문자열)/주석문 분석	문자열 [탐색] 분석 도구	https://github.com/nextB/scancode-toolkit
NinKa	AGPL-3.0	소스코드 파일 내 라이선스 고지 문구(문자열)/주석문 분석	문자열 [탐색] 분석 도구	https://ninka.turingmachine.org/
TripleCheck	AGPL-3.0	소스코드 파일 내 라이선스 고지 문구(문자열)/주석문 분석	문자열 [탐색] 분석 도구	https://triplecheck.net/download.html

IV. 결론

IoT, 빅데이터, 로봇, AI는 물론 ERP, 게임, 보안, 클라우드, 가상화 등 다양한 분야에서 OSS의 활용은 계속 증가하고 있다. 무엇보다도 빠른 기술 변화 속도에 대한 대응과 비용 절감이 가능하다는 점이 OSS 활용 목적의 가장 큰 이유이기도 하지만 기술 종속성 탈피와 OSS의 품질 수준도 뒤따르기 때문에 기술 개발에서 더 많은 OSS의 사용과 활성화가 증대되는 것이다.

대표적인 OSS 기반 제품으로는, OS 분야에서는 Redhat과 CentOS, WEB/WAS 분야에서는 Apache, Tomcat, Jboss, DB 분야에서는 PostgreSQL/PAS, MariaDB/MySQL이 있다. 이

외에도 솔루션 분야에서의 ALM(Application Life Cycle Management)과 개발 언어에서 Python과 Perl, 개발 도구로 사용하는 Eclipse 등이 OSS가 활용되어 만든 오픈소스 기반 제품들이다.

앞으로 기업과 공공기관에서의 기술 및 제품 개발에 있어서 OSS의 활용은 더욱 증가될 전망이다. 이에 본 고에서는 OSS 활용 증대에 따라 필요한 국내외 기업의 OSS 거버넌스 동향을 조사하고, 나아가 SW 개발 과정에서 OSS 사용에 앞서 사전 검토가 필요한 주요 OSS 라이선스의 내용과 라이선스 분석 및 검증을 위해 사용 가능한 자동화 툴 동향을 살펴보았다. 따라서 본 고가 앞으로 기업이나 공공기관에서의 OSS 활용 증대에 따른 OSS 거버넌스 준비와 방향에 도움이 될 수 있기를 기대한다.

[참고문헌]

- [1] NIPA, “공개 SW라이선스 가이드”, 2017. 1.
- [2] KCC(한국저작권위원회), “오픈소스소프트웨어 라이선스 가이드 3.0”, 2016. 11.
- [3] Black Duck Korea, “OSS 라이선스 이해 및 관리”, ETRI Seminar, 2017. 8.
- [4] NIPA, “제5회 공개 SW 거버넌스 아카데미”, 2018. 6.
- [5] NIPA, “제6회 공개 SW 거버넌스 아카데미”, 2018. 7.
- [6] NIPA, “공공 공개 SW 거버넌스 가이드”, 2017.1.
- [7] NIPA, “공개소프트웨어 거버넌스 프레임워크 및 적용가이드”, 2015. 8.
- [8] 정보통신부, “공공기관을 위한 공개소프트웨어안내서, 2005.
- [9] ETRI, 오픈소스 SW 대응 추진 계획, 2017. 5.

* 본 고는 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원((R7119-16-1001, 지식증강형 실시간 동시통역 원천기술 개발), (2013-2-00131, (엑소브레인-1세부) 휴먼 지식증강 서비스를 위한 지능진화형 WiseQA 플랫폼 기술 개발)을 받아 수행한 연구 결과임/본 연구 결과는 ETRI 공식 견해와 다를 수 있음