BLACKDUCK

오픈소스 라이선스 이해와 관리

2016.08.25

블랙덕소프트웨어코리아

© 2016. Black Duck Software Korea all rights reserved.

CONTENTS

1. 오픈소스 동향

2. 오픈소스 개념 및 라이선스 이해

3. 오픈소스 라이선스 관리와 위반사례

4. Black Duck Suite

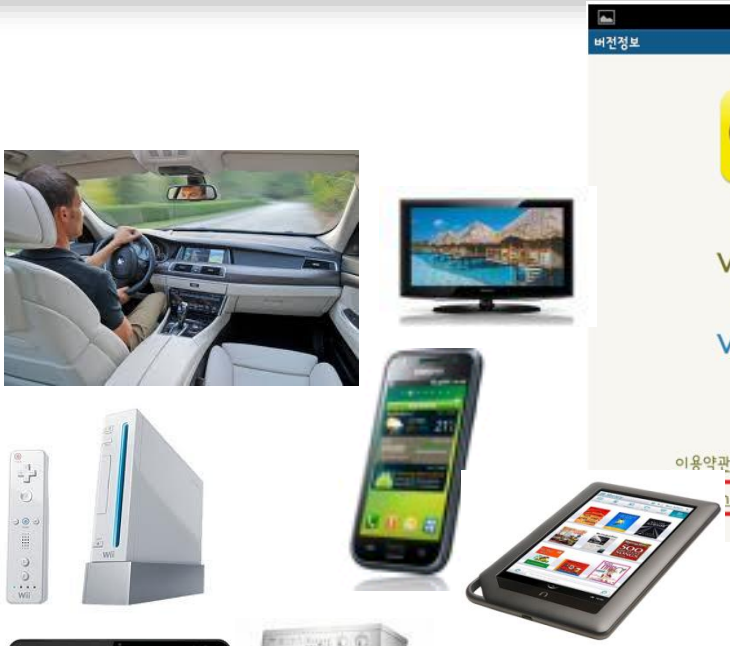
© 2016. Black Duck Software Korea all rights reserved.

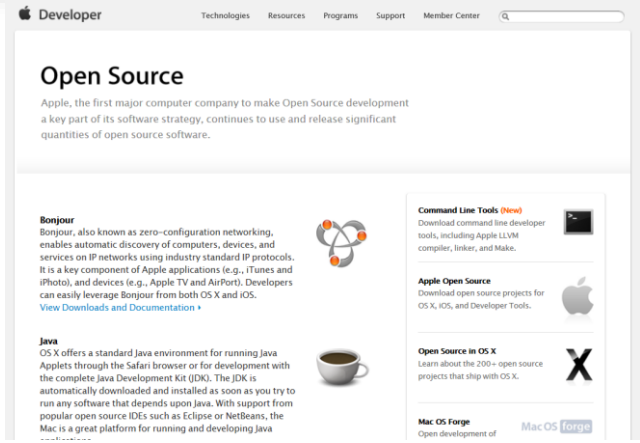
BLACKDUCK

1. 오픈소스 동향

© 2016. Black Duck Software Korea all rights reserved.

오픈소스 혁명





Android(Google)

iOS(Apple)

ChromeOS(Google)

Tizen(Linux Foundation, LiMo+MeeGo)

GENIVI Alliance :

Open In Vehicle Infotainment 플랫폼

Tajo

© 2016. Black Duck Software Korea all rights reserved.

BLACKDUCK

오픈소스의 활용

▣ 오픈소스는 소스코드, 라이브러리, 유틸리티, 툴, 완제품 수준에 이르기 까지 다양한 방법으로 활용 될 수 있음

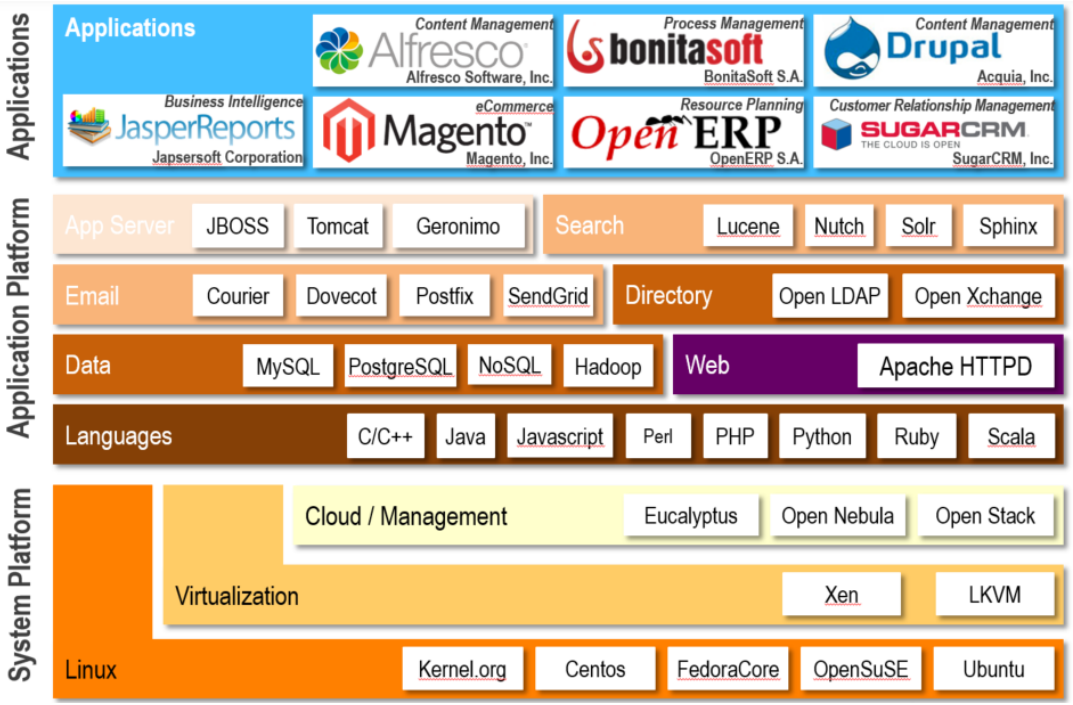
▣ 특히, 다양한 오픈소스를 활용함에 있어서는 결합형태에 따라 소스코드 공개 범위가 상이할 수 있어 결합형태에 따른 라이선스 호환성 검토를 수행해야 하며, 라이선스 이슈는 보통 소스 코드와 라이브러리 수준의 결합 형태에서 많이 발생 됨

※ AGPL은 완제품 수준에서 이슈가 발생함

활용 단위

- **소스코드**
- **라이브러리**
- 유틸리티
- 툴(개발, 관리, 테스트)
- 완제품

분류 체계



© 2016. Black Duck Software Korea all rights reserved.

BLACKDUCK

슈퍼 오픈소스 커뮤니티

Financial Services

THE LODESTONE FOUNDATION
Open Source for Capital Markets and Beyond

OpenMAMA

Mobile

Healthcare

OSEHRA
Open Source Electronic Health Record Agent

Automotive

GENIVI

Aerospace

Polarsys

Openstack

The Apache Foundation

Mozilla

The LINUX Foundation

Eclipse

© 2016. Black Duck Software Korea all rights reserved.

BLACKDUCK

오픈소스 관련 단체

- **Free Software Foundation**
  - **리처드 스톨만**에 의해 1985년 만들어진 비영리 재단
  - GNU프로젝트 운영 및 Free SW 배포/관리 단체
- **OSI (Open Source Initiative)**
  - 오픈 소스 소프트웨어 사용 장려를 위해 만들어진 단체
  - **오픈 소스 소프트웨어 정의** 및 관련 표준 관리
- **SFLC (Software Freedom Law Center)**
  - 자유 소프트웨어 / 오픈 소스 소프트웨어의 비영리 개발자를 위하여 법률 상담 법률 대리 및 관련 서비스
  - **에벤 모글 렌** 의장이 2005년 2월에 4백만달러 달러의 초기 자금으로 오픈 소스 개발 연구소를 위하여 설립
- **GPL Violation**
  - **해럴드 벨테**에 의해 2004년 만들어진 비영리 재단
  - GPL 라이선스 기반의 저작권 보호 및 소송지원 단체
- **기타 – Linux Foundation, FOSS, OIN 등**

FREE SOFTWARE FOUNDATION

open source

frdm

Let's save the GNU!
gpl-violations.org

openinventionnetwork

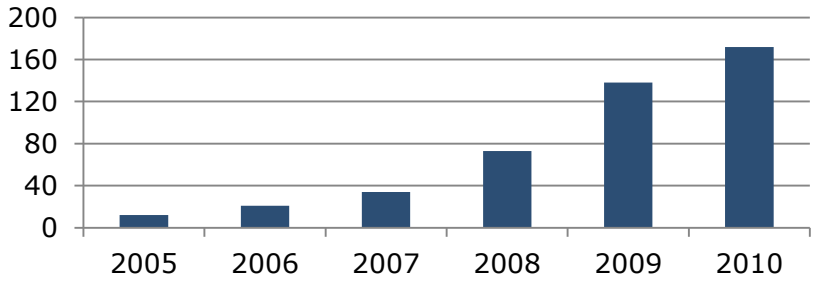
© 2016. Black Duck Software Korea all rights reserved.

BLACKDUCK

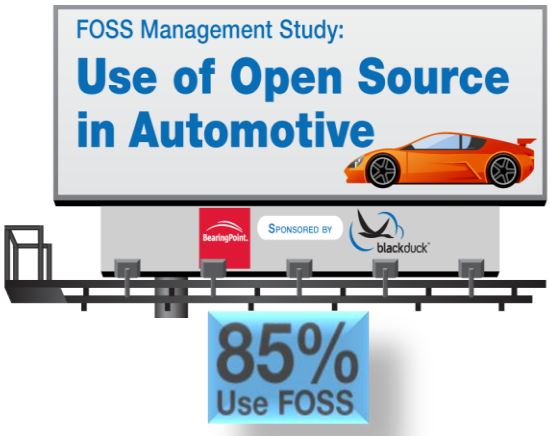
오픈소스 프로젝트 개발 및 사용현황

- 2011년에만 Mobile 분야에서 10,000개 이상의 신규 오픈소스 프로젝트 개발, 안드로이드 플랫폼 기반이 76%
- 클라우드 오픈소스 프로젝트도 연평균 75%로 급속도로 증가하고 있음
- Bearing Point에서 조사한 Automotive OSS Study 2012에 의하면 자동차 산업에서 약 85% 오픈소스 사용

New Cloud OSS Projects

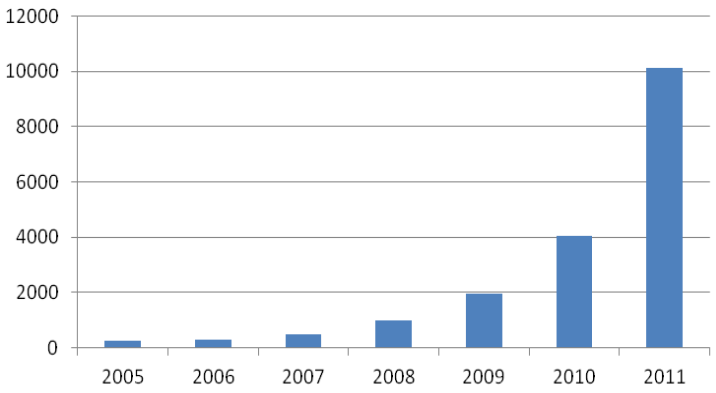


- >450 cumulative projects
- 75% CAGR
- Diverse technologies



- >18,000 cumulative projects
- 2X growth each of last 3 years
- 10,000 new in 2011 alone!

New Mobile OSS Projects

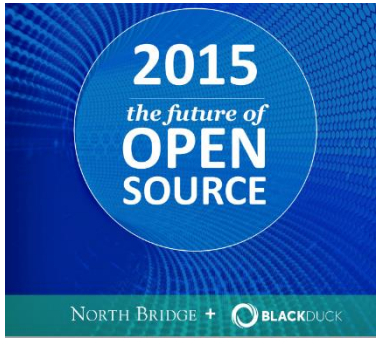


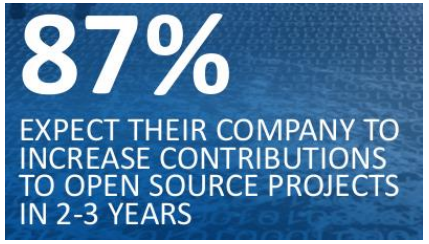
Bearing Point Automotive OSS Study 2012

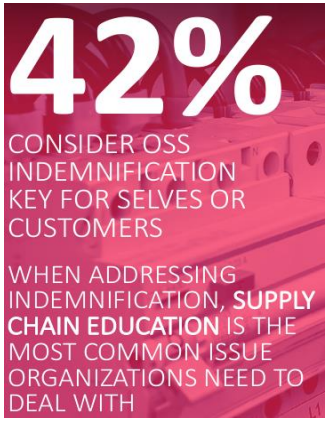
© 2016. Black Duck Software Korea all rights reserved.
BLACKDUCK

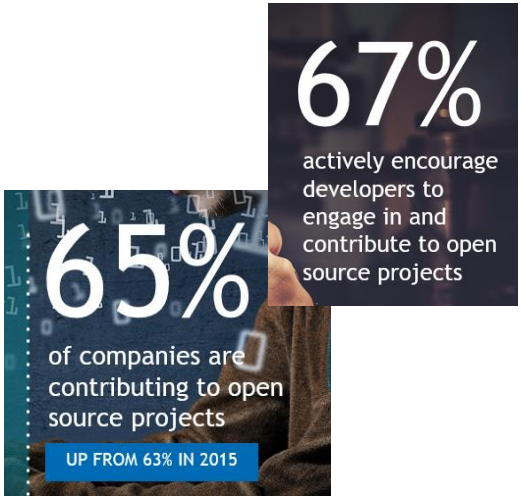
오픈소스 트랜드(Enterprise Adoption)

- North Bridge와 Black Duck이 1,300 명의 다양한 IT기업 임직원들을 대상으로 실시한 the future of Open Source 2015, 2016 리서치 결과에에 의하면 78%의 기업들이 오픈소스를 사용, 67%의 기업들이 개발자들에게 오픈소스 참여를 장려, 65%가 오픈소스 프로젝트에 참여하고 있으며, 향후 2-3년 이내에 87%가 오픈소스 프로젝트에 참여할 것으로 기대
- 특히, 42%가 내부적으로나 고객을 위해 오픈소스 배상(면책)을 중요하게 검토하고 있음
- 오픈소스의 사용과 참여가 획기적으로 증가하고 있음





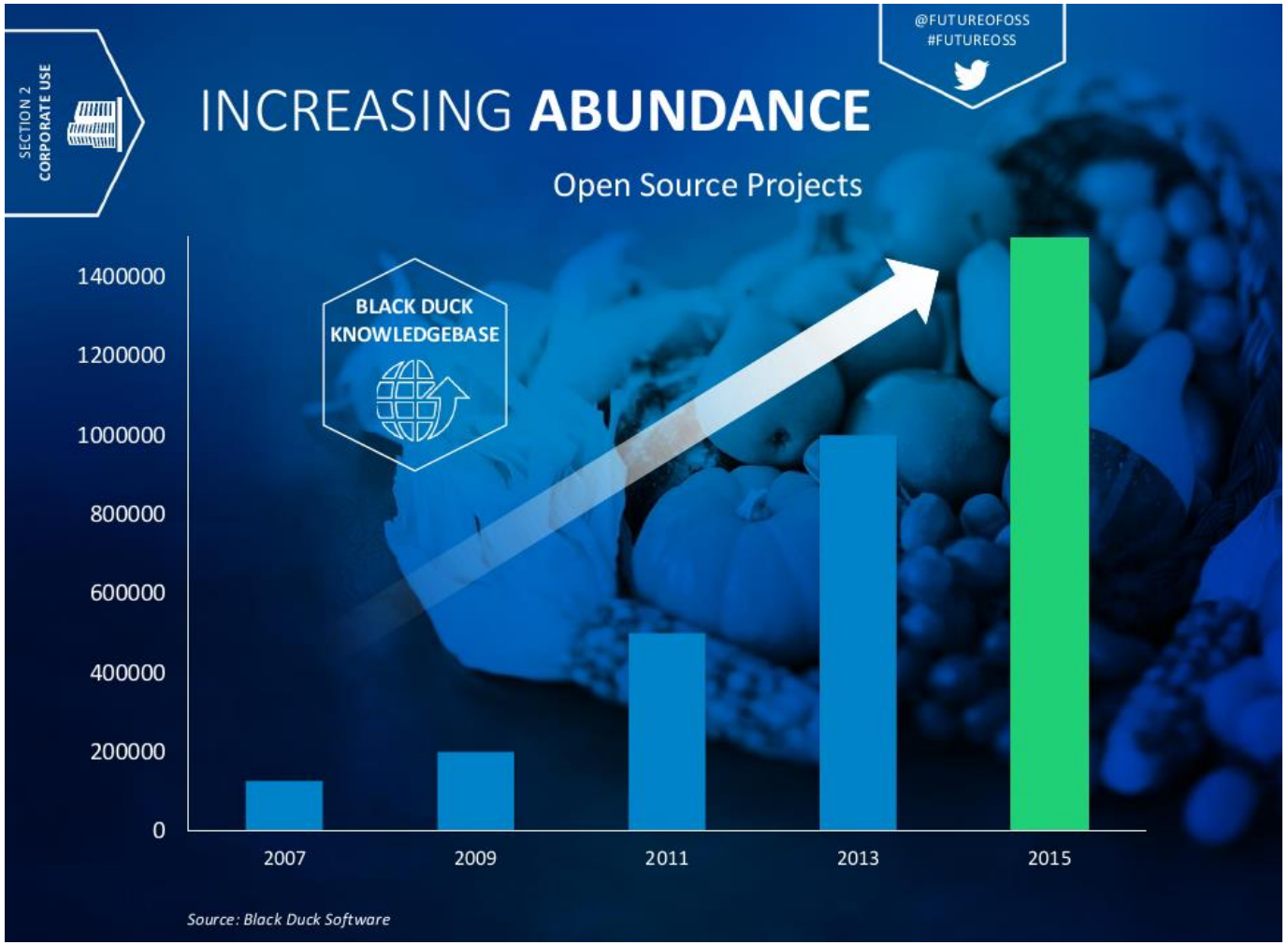




© 2016. Black Duck Software Korea all rights reserved.

오픈소스 프로젝트 개발 및 사용현황

▣ 블랙덕 오픈소스 DB 기준으로 픈소스 프로젝트가 기하 급수적으로 증가하고 있음



© 2016. Black Duck Software Korea all rights reserved.

자동차 산업에서의 오픈소스 현황

Black Duck Software & Bearing Point Automotive OSS Study 2012

© 2016. Black Duck Software Korea all rights reserved.

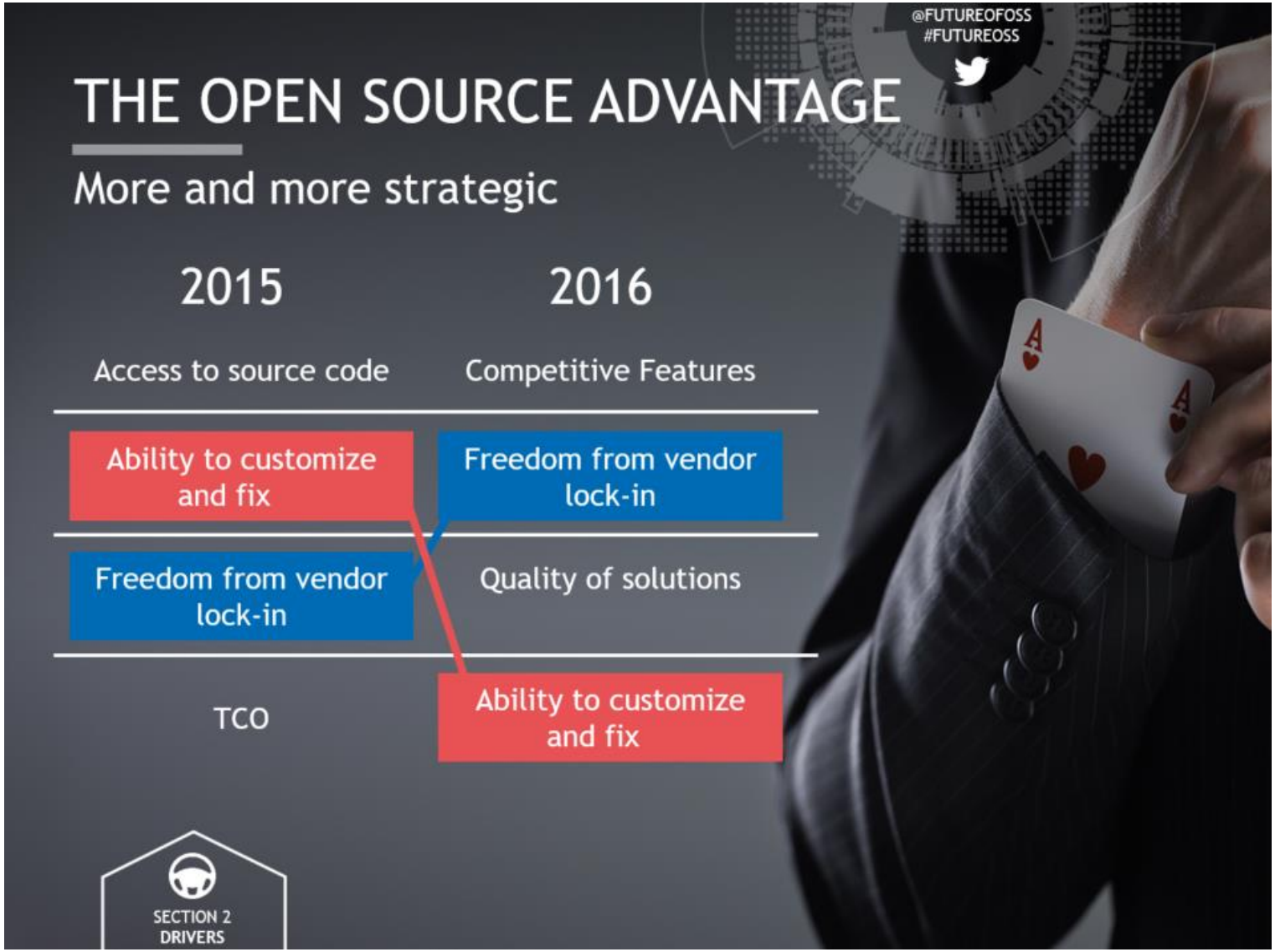
오픈소스 프로젝트 개발 및 사용현황

© 2016. Black Duck Software Korea all rights reserved.

오픈소스 채택 이유

© 2016. Black Duck Software Korea all rights reserved.

오픈소스 채택 이유



© 2016. Black Duck Software Korea all rights reserved.

오픈소스 핵심산업

© 2016. Black Duck Software Korea all rights reserved.

BLACKDUCK

국내 오픈소스 표준화 정책

▣ 2014년 TTA PG602(공개소프트웨어 프로젝트그룹) 에서 추진한 공개소프트웨어 거버넌스 프레임워크가 정보통신단체표준으로 채택, 현재 SPDX 단체 표준을 추진하고 있음.

표준종류	정보통신단체표준(TTAS)		
표준번호	TTAK.KO-11.0176	구 표준번호	
제개정일	2014-07-02	총페이지	19
한글 표준명	공개소프트웨어 거버넌스 프레임워크		
영문 표준명	The Governance framework for Open Source Software		
한글 내용요약	공개 소프트웨어 거버넌스 프레임워크는 조직을 중심으로 한 공개 소프트웨어의 흐름에 따라 세 단계로 분류된다. 첫 번째 단계는 공개 소프트웨어를 조직 내에서 사용하는 내부 사용에 해당된다. 두 번째 단계는 공개 소프트웨어를 조직 밖으로 보내는 배포 과정이다. 마지막은 조직이 공개 소프트웨어 사용자에게 기술 지원 서비스를 제공하는 외부 서비스 단계이다. 실행 항목 및 검사 목록들은 각 단계의 특성에 따라서 공개 소프트웨어 거버넌스에 대한 표준 요소로 정의된다.		
영문 내용요약	이 표준은 주로 소프트웨어 산업계, 정부 부처와 관련돼 있다. 주요 수혜자는 공개 소프트웨어 사용자로서 회사, 정부, 준법성 위반을 감시하는 법무 조직, 그리고 공개 소프트웨어 서비스 제공자 등이 포함된다. 이 표준은 소프트웨어 분야 전반에서 공개 소프트웨어가 안정성을 갖고 최대한 폭 넓게 적용되는 데 기여할 것으로 여겨진다.		
관련 IPR 확약서	접수된 IPR 확약서 없음		

[출처] http://www.tta.or.kr/data/ttas_view.jsp?rn=1&rn1=Y&rn2=&rn3=&nowpage=1&pk_num=TTAK.KO-11.0176&standard_no=&kor_standard=%B0%C5%B9%F6%B3%CD%BD%BA&publish_date=&section_code=&order=publish_date&by=desc&nowSu=1&totalSu=8&acode1=&acode2=&scode1=&scode2=

© 2016. Black Duck Software Korea all rights reserved.

오픈소스 공급망 관리를 위한 표준

▣ 표준
- 소프트웨어 패키지 관련 콤포넌트, 라이선스, copyrights, 사용 파일의 CheckSum 정보 등을 상호 교환하기 위한 표준
- Linux Foundation의 오픈 컴플라이언스 프로그램의 핵심

▣ SPDX Group:
- Linux Foundation의 워킹그룹
- 삼성전자 포함 50여 개 이상의 소프트웨어, 시스템, 툴 벤더, 컨설턴트 등이 참여

▣ 소프트웨어 패키지에 포함된 실제 파일의 라이선스 정보를 설명하기 위한 정의된 표준화된 포맷

▣ 현재 버전2.0이 출시

▣ 인텔, 필립스 등 SPDX를 통한 공급망 관리 시행 중

SPDX®

SOFTWARE PACKAGE DATA EXCHANGE®

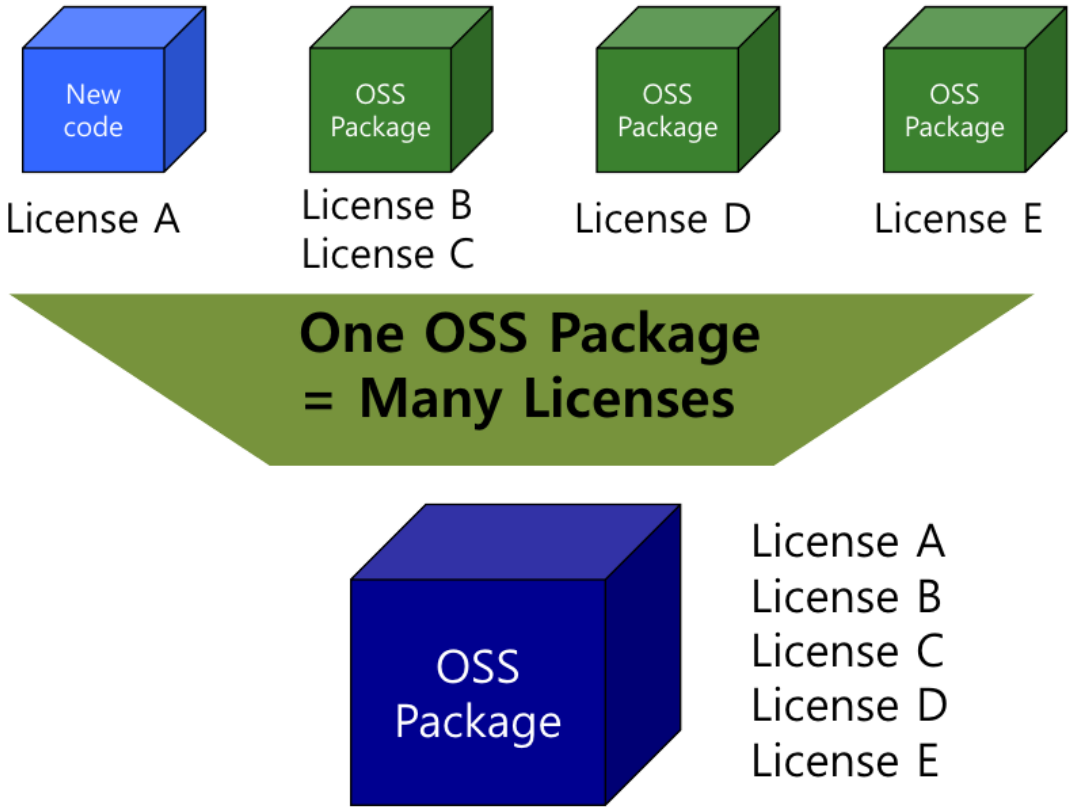
See: http://www.spdx.org
Getting started - http://spdx.org/wiki/spdx/participation-guidelines

Contact:
General - Phil Odence (Chair) - podence@blackducksoftware.com
Business team - Jack Manbeck (Co-Chair)- j-manbeck2@ti.com
Legal team - Jilayne Lovejoy (Co-Chair) - jilayne.lovejoy@openlogic.com
Technical team - Kate Stewart (Chair) - stewart@linux.com

© 2016. Black Duck Software Korea all rights reserved.

SPDX (Software Package Data Exchange)

- An OSS Package can contain multiple OSS packages, multiple licenses.



License info for OSS is not provided in a consistent, easy-to-use format

12

[출처] 삼성전자 2014 삼성 오픈소스 컨퍼런스 발표자료 : Introduction to SPDX for Better Compliance

© 2016. Black Duck Software Korea all rights reserved.

국내 오픈소스 관리 및 장려정책

▣ 2011년 부터 정보통신산업진흥원 공개SW 역량프라자에서 국내 중소기업 및 개발자 개인, 학교 및 비영리 연구기관을 대상으로 무료 오픈소스 라이선스 검증서비스를 지원

- http://www.oss.kr/oss_business9_2 검증서비스 신청
- 프로젝트 별 소스코드 500MB이하 단위로 신청할 수 있으며 총3회까지 신청가능

© 2016. Black Duck Software Korea all rights reserved.

2. 오픈소스 개념 및 라이선스 이해

© 2016. Black Duck Software Korea all rights reserved.

BLACKDUCK

오픈소스의 정의

- 오픈소스와 상용 소프트웨어의 가장 큰 공통점은 저작권이 있다는 것
- 다만, 저작권리의 행사방식이 가장 큰 차이점이며 일반적인 오픈소스 저작권자들은 소스 코드를 공개하고 누구나 복제, 설치, 사용, 변경, 재배포가 가능하도록 저작권리를 행사하고 있음

일반적인 오픈소스 코드

```
See http://www.astray.com/acmemail/

acmemail is Copyright (c) 1997-2000 Leon Brocard. All rights reserved.
portions Copyright (c) 2001 Peter Watkins

You may distribute acmemail under the terms of either the GNU General  Public License as published by
the Free Software Foundation (either version 2 of the
License or at your option any  later version) or the
Artistic License. You should have received a copy of both licenses along with this program.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the
implied warranty of MERCHANTABILITY or FITNESS FOR A
PARTICULAR PURPOSE.  See the GNU General Public License
For more details. Version: see acme_version() in AcmemailConf.pm

Include any library directories

use lib '.';
#use lib '/lib/place‘;
```


© 2016. Black Duck Software Korea all rights reserved.

Open Source Initiative 오픈소스 정의

http://opensource.org/

'15년 현재 Apache, MIT 등 총 83개의 OSI 인증 라이선스

Introduction

Open source doesn't just mean access to the source code. The distribution terms of open-source software must comply with the following criteria:

1. Free Redistribution 자유로운 재배포

The license shall not restrict any party from selling or giving away the software as a component of an aggregate software distribution containing programs from several different sources. The license shall not require a royalty or other fee for such sale.

2. Source Code 원시코드 제공

The program must include source code, and must allow distribution in source code as well as compiled form. Where some form of a product is not distributed with source code, there must be a well-publicized means of obtaining the source code for no more than a reasonable reproduction cost preferably, downloading via the Internet without charge. The source code must be the preferred form in which a programmer would modify the program. Deliberately obfuscated source code is not allowed. Intermediate forms such as the output of a preprocessor or translator are not allowed.

3. Derived Works 파생저작물

The license must allow modifications and derived works, and must allow them to be distributed under the same terms as the license of the original software.

4. Integrity of The Author's Source Code 저작자의 소스코드 원형 유지: 최초 원시코드 & 패치

The license may restrict source-code from being distributed in modified form *only* if the license allows the distribution of "patch files" with the source code for the purpose of modifying th integrity at build time. The license must explicitly permit distribution of software built from modified source code. The license may require derived works to carry a different name or version number from the original software.

5. No Discrimination Against Persons or Groups 개인 및 단체에 대한 차별 금지

The license must not discriminate against any person or group of persons.

6. No Discrimination Against Fields of Endeavor 사용 분야에 대한 차별 금지

The license must not restrict anyone from making use of the program in a specific field of endeavor. For example, it may not restrict the program from being used in a business, or from being used for genetic research.

7. Distribution of License 라이선스의 배포

The rights attached to the program must apply to all to whom the program is redistributed without the need for execution of an additional license by those parties.

8. License Must Not Be Specific to a Product 특정 제품에만 유효한 라이선스 금지

The rights attached to the program must not depend on the program's being part of a particular software distribution. If the program is extracted from that distribution and used or distributed within the terms of the program's license, all parties to whom the program is redistributed should have the same rights as those that are granted in conjunction with the original software distribution.

9. License Must Not Restrict Other Software 다른 소프트웨어를 제한하는 라이선스 금지

The license must not place restrictions on other software that is distributed along with the licensed software. For example, the license must not insist that all other programs distributed on the same medium must be open-source software.

10. License Must Be Technology-Neutral 라이선스의 기술 중립성

No provision of the license may be predicated on any individual technology or style of interface.

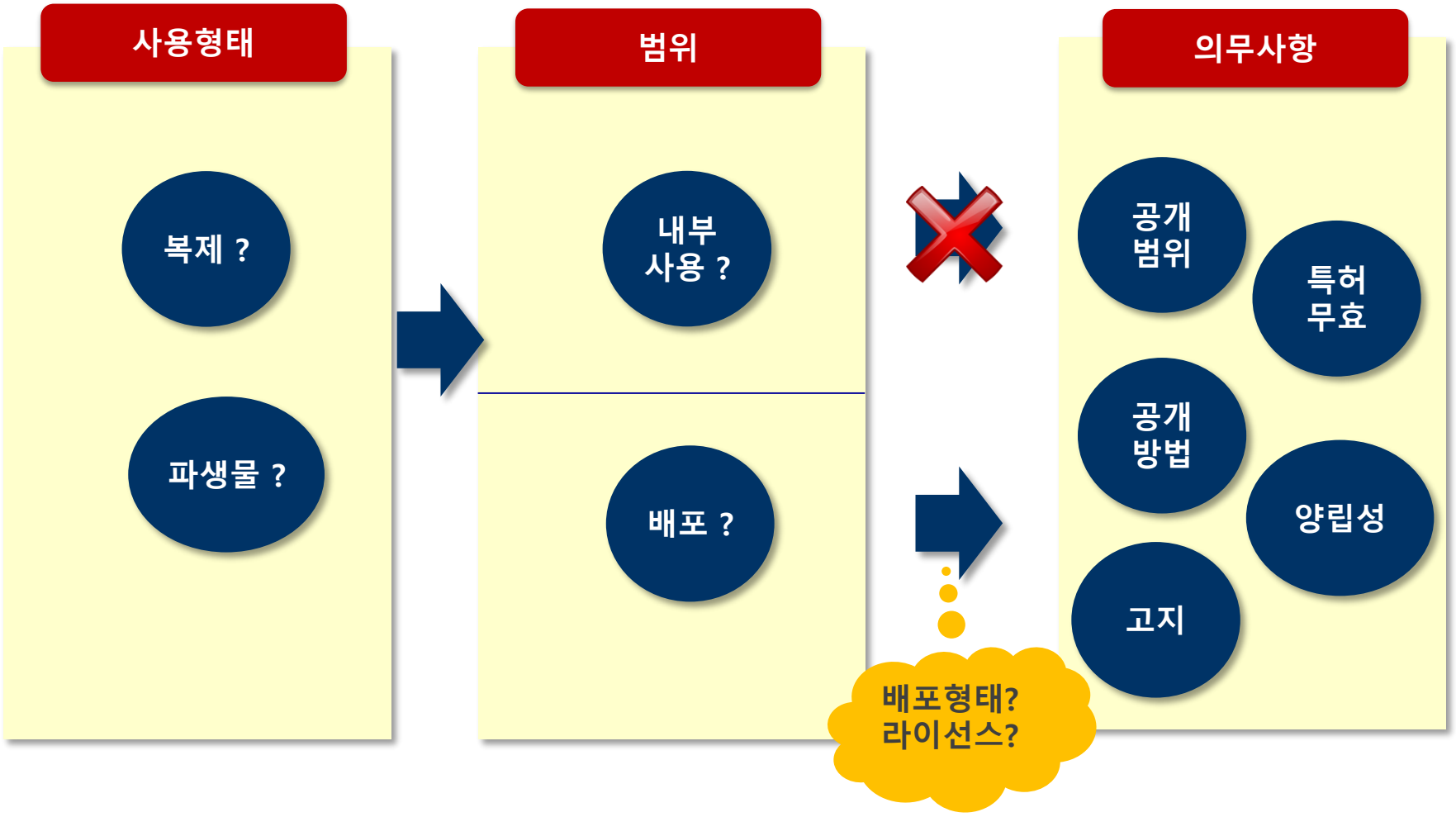
© 2016. Black Duck Software Korea all rights reserved.

Open Source Initiative 인증 83개 오픈소스 라이선스

Academic Free License 3.0 (AFL-3.0)
Affero GNU Public License: See *"GNU Affero General Public License 3.0 (AGPL-3.0)"*
Adaptive Public License (APL-1.0)
Apache License 2.0 (Apache-2.0)
Apple Public Source License (APSL-2.0)
Artistic license 2.0 (Artistic-2.0)
Attribution Assurance Licenses (AAL)
BSD 3-Clause "New" or "Revised" License (BSD-3-Clause)
BSD 2-Clause "Simplified" or "FreeBSD" License (BSD-2-Clause)
Boost Software License (BSL-1.0)
Computer Associates Trusted Open Source License 1.1 (CATOSL-1.1)
Common Development and Distribution License 1.0 (CDDL-1.0)
Common Public Attribution License 1.0 (CPAL-1.0)
CUA Office Public License Version 1.0 (CUA-OPL-1.0)
EU DataGrid Software License (EUDatagrid)
Eclipse Public License 1.0 (EPL-1.0)
Educational Community License, Version 2.0 (ECL-2.0)
Eiffel Forum License V2.0 (EFL-2.0)
Entessa Public License (Entessa)
European Union Public License, Version 1.1 (EUPL-1.1) *(links to every language's version on their site)*
Fair License (FAIR)
Frameworx License (Frameworx-1.0)
GNU Affero General Public License v3 (AGPL-3.0)
GNU General Public License version 2.0 (GPL-2.0)
GNU General Public License version 3.0 (GPL-3.0)
GNU Library or "Lesser" General Public License version 2.1 (LGPL-2.1)
GNU Library or "Lesser" General Public License version 3.0 (LGPL-3.0)
Historical Permission Notice and Disclaimer (HPND)
IBM Public License 1.0 (IPL-1.0)
IPA Font License (IPA)
ISC License (ISC)
LaTeX Project Public License 1.3c (LPPL-1.3c)
Lucent Public License Version 1.02 (LPL-1.02)
MirOS Licence (MirOS)
Microsoft Public License (Ms-PL)
Microsoft Reciprocal License (Ms-RL)
MIT license (MIT)
Motosoto License (Motosoto)
Mozilla Public License 2.0 (MPL-2.0)
Multics License (Multics)
NASA Open Source Agreement 1.3 (NASA 1.3)
NTP License (NTP)
Naumen Public License (Naumen)
Nethack General Public License (NGPL)
Nokia Open Source License (Nokia)
Non-Profit Open Software License 3.0 (NPOSL-3.0)
OCLC Research Public License 2.0 (OCLC-2.0)
Open Font License 1.1 (OFL 1.1)
Open Group Test Suite License (OGTSL)
Open Software License 3.0 (OSL-3.0)
PHP License 3.0 (PHP-3.0)
The PostgreSQL License (PostgreSQL)
Python License (Python-2.0) (overall Python license)
CNRI Python license (CNRI-Python) (CNRI portion of Python License)
Q Public License (QPL-1.0)
RealNetworks Public Source License V1.0 (RPSL-1.0)
Reciprocal Public License 1.5 (RPL-1.5)
Ricoh Source Code Public License (RSCPL)
Simple Public License 2.0 (SimPL-2.0)
Sleepycat License (Sleepycat)
Sun Public License 1.0 (SPL-1.0)
Sybase Open Watcom Public License 1.0 (Watcom-1.0)
University of Illinois/NCSA Open Source License (NCSA)
Vovida Software License v. 1.0 (VSL-1.0)
W3C License (W3C)
wxWindows Library License (WXwindows)
X.Net License (Xnet)
Zope Public License 2.0 (ZPL-2.0)
zlib/libpng license (Zlib)

© 2016. Black Duck Software Korea all rights reserved.

오픈소스 라이선스 주요 용어 및 개념



© 2016. Black Duck Software Korea all rights reserved.

라이선스 개념 분류

오픈소스와 비오픈소스의 차이

Non-Open Source Software

Open Source Software

Free Software

- 프로그램을 실행할 수 있는 자유
- 프로그램을 채택하고 연구할 수 있는 자유
- 프로그램을 재 배포 할 수 있는 자유
- 프로그램을 개선할 수 있는 자유

FREE SOFTWARE FOUNDATION

Richard Stallman, 1983

Open Source Software

- 개발되는 방식에 초점을 추는 실용적 접근
- 산업계는 물론이고 개발자에게도 경제적인 보상을 할 수 있어야 한다고 주장
- "보는 눈만 많다면, 어떤 버그라도 쉽게 잡을 수 있다"

open source

Eric Raymond, 1998

© 2016. Black Duck Software Korea all rights reserved.

BLACKDUCK

라이선스 개념 분류

Permissive	Copyleft
▪ 사용함에 있어서 별다른 요구사항을 부여하지 않고 광범위한 권한을 부여 ▪ 라이선스 요구사항 최소화 (라이선스 copy, notice보전)	▪ 소스코드가 사용되어 지게 해야 함. ▪ 라이선스는 원래 저작물과 그에 따른 파생저작물에 적용되어 져야 함.

Free Software/ Opens Source Software ?

Free Opens Source Software ?

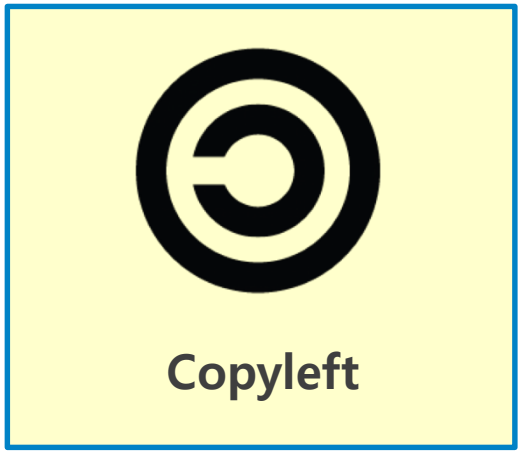
- **Give Me Credit**
  - ➢ **BSD, MIT**
- **Give Me Fixes**
  - ➢ **MPL, EPL, LGPL**
- **Give Me Everything**
  - ➢ **GPL**

© 2016. Black Duck Software Korea all rights reserved.
BLACKDUCK

Free Software 정의

Free : 아무 이유 없는 자유
Freedom : 자유와 권리가 함께 주어지며 권리에 따른 책임이 부여되는 자유

- ▣ 프로그램을 실행할 수 있는 자유
- ▣ 프로그램을 채택하고 연구할 수 있는 자유
- ▣ 프로그램을 재배포 할 수 있는 자유
- ▣ 프로그램을 개선할 수 있는 자유



Free Software / Opens Source Software ?

Making Sense of Open Source Licenses by J Aaron Farr ApacheCon US 2009

© 2016. Black Duck Software Korea all rights reserved.

라이선스 사용빈도 TOP 20

Rank	License	%
1.	MIT License	26%
2.	**GNU General Public License (GPL) 2.0**	**21%**
3.	Apache License 2.0	16%
4.	**GNU General Public License (GPL) 3.0**	**9%**
5.	BSD License 2.0 (3-clause, New or Revised) License	6%
6.	**GNU Lesser General Public License (LGPL) 2.1**	**4%**
7.	Artistic License (Perl)	4%
8.	**GNU Lesser General Public License (LGPL) 3.0**	**2%**
9.	ISC License	2%
10.	Microsoft Public License	2%
11.	**Eclipse Public License (EPL)**	**1%**
12.	Code Project Open License 1.02	< 1%
13.	**Mozilla Public License (MPL) 1.1**	**< 1%**
14.	Simplified BSD License (BSD)	< 1%
15.	**Common Development and Distribution License (CDDL)**	**< 1%**
16.	**GNU Affero General Public License v3 or later**	**< 1%**
17.	Microsoft Reciprocal License	< 1%
18.	Sun GPL With Classpath Exception v2.0	< 1%
19.	DO WHAT THE FUCK YOU WANT TO PUBLIC LICENSE	< 1%
20.	CDDL-1.1	< 1%

[출처] Black Duck Software, Inc 2016년 현재

© 2016. Black Duck Software Korea all rights reserved.

주요 라이선스 및 의무사항

▣ 주요 오픈소스 라이선스인 GPL, LGPL, CPL, MPL 등은 오픈소스 코드 뿐 아니라 사용자 코드 공개의무 발생

▣ 오픈소스를 활용하면서 공개하기 어려운 코드를 보호하기 위해서는 적절한 라이선스 관리가 필요함

라이선스	주요 의무사항	공개 범위 및 특징
GPL (General Public License)	▪ 자유로운 사용, 복제, 배포 및 수정 ▪ 저작권 표시, 보증책임이 없다는 표시, GPL 명시 ▪ 소프트웨어 수정 및 링크 시 모든 코드를 GPL에 의해 공개	▪ GPL 코드와 연결된 모든 코드
LGPL (Lesser General Public License)	▪ 자유로운 사용, 복제, 배포 및 수정 ▪ 저작권 표시, 보증책임이 없다는 표시, LGPL 명시 ▪ 소프트웨어 수정 및 링크 시 모든 코드를 LGPL에 의해 공개 (단, 라이브러리 링크 시 공개하지 않음)	▪ LGPL 코드와 연결된 모든 코드
MPL (Mozilla Public License)	▪ 자유로운 사용, 복제, 배포 및 수정 ▪ 저작권 표시, 보증책임이 없다는 표시, MPL 명시 ▪ 특허 보복조항(특허 SW사용시 특허권을 주장할 수 없음) ▪ 소프트웨어 수정 및 링크 시 해당 파일을 공개	▪ MPL 코드와 연결된 해당 파일
EPL (Eclipse Public License)	▪ 자유로운 사용, 복제, 배포 및 수정 ▪ 저작권 표시, 보증책임이 없다는 표시, MPL 명시 ▪ 특허 보복조항(특허 SW사용시 특허권을 주장할 수 없음) ▪ 소프트웨어 수정 및 링크 시 해당 모듈을 공개	▪ EPL 코드와 연결된 해당 모듈 ▪ 특허 SW시 특허권리 주장 하지 못함

© 2016. Black Duck Software Korea all rights reserved.

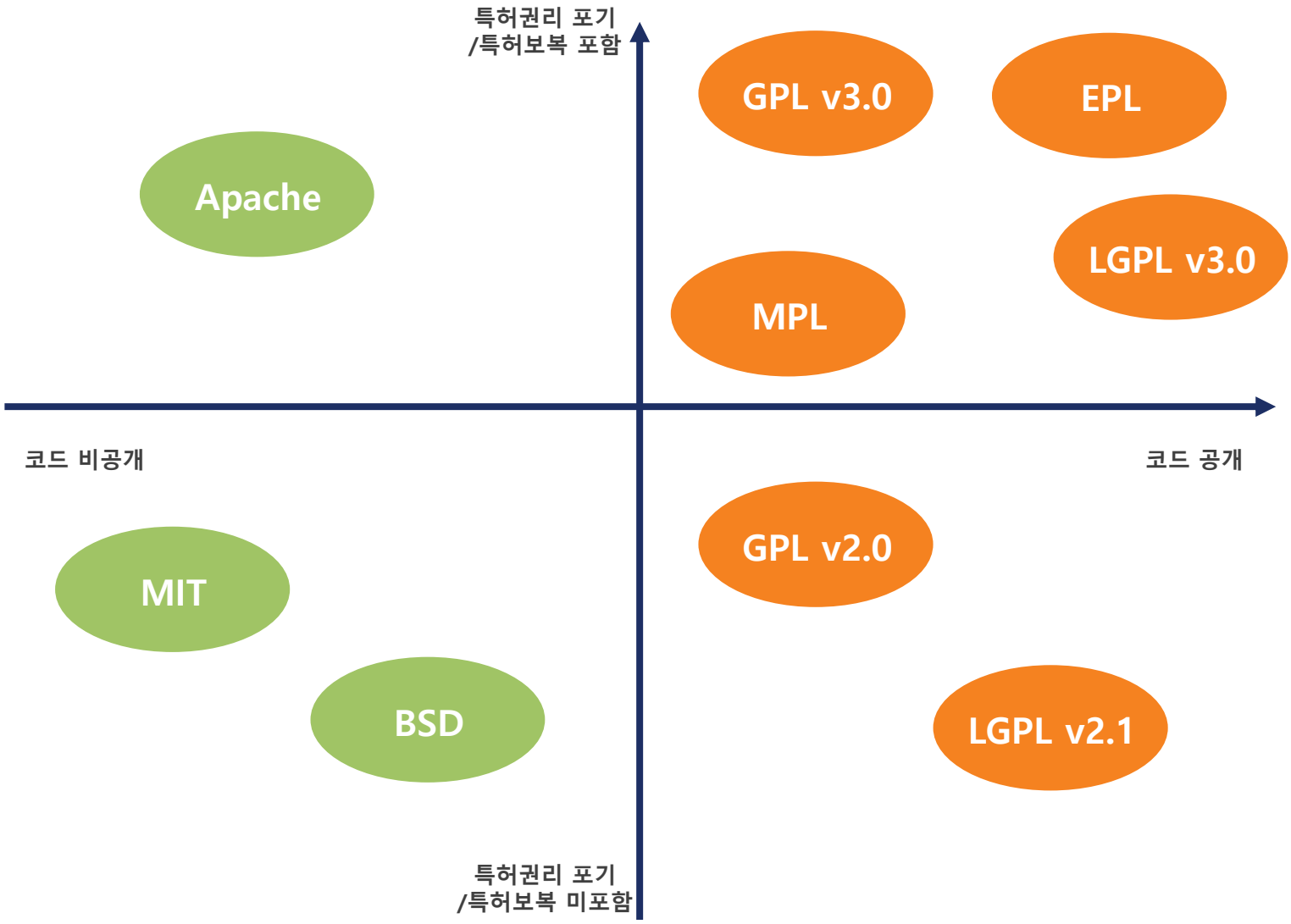
GPL의 주요특징

- 1989년 GPL 1.0 버전이 FSF(리처드 스톨만)에서 만들어짐
- 1991년 6월 GPL 2 발표
- 2006년 초 GPL 3 초안발표
- 2007년 6월에 GPL 3 정식버전이 발표됨

라이선스 조항	GPL 2.0 의무사항	GPL 3.0 의무사항
Patent Retaliation (특허보복 조항)	본 항목은 특허보복조항이 있는가 하는 것으로 특정 개인 및 단체에 대한 보복조항과 프로그램 관련 특허 보복조항으로 구분하고 있음. GPL 2.0은 어떠한 특허 보복조항도 없음.	GPL 3.0에서는 특허에 대한 보복조항이 있어 특허 소송을 제기할 경우 저작권 라이선스 뿐 아니라 특허라이선스까지 자동종료되게 됨.
Express Patent License (특허 라이선스 명시)	명시적으로 보유한 특허에 대한 무상실시 권을 부여하거나 소제기를 하지 않는다는 조항은 없음.	GPL 3.0에서는 명시적 특허라이선스 조항이 있고 특허 라이선스의 내용에 대해 특허 침해 청구를 하지 않는 것이라고 명확하게 말하고 있음.
Anti-DRM Provisions (DRM금지 조항)	GPL 2.0에서는 DRM에 대한 내용을 다루고 있지 않음.	제3조에서 기술적 회피 금지법의 적용을 받지 않는다는 점을 명확히 하고 있어 DRM 금지조항을 가지고 있음.
Share-alike / Reciprocity (공유)	제0조와 제2조에서 원 프로그램 뿐 아니라 원 프로그램에 기반한 프로그램도 동일한 라이선스의 적용을 받는 것으로 되어 있음.	제5조와 제6조에서는 변경한 부분에 대해서도 동일한 조건을 적용하여야 한다는 조항이 있음. 다만 제13조에서 AGPL적용 저작물과 결합할 경우, 그 결합물 전체에 대해서는 GPL3.0이 적용되지만, 네트웍을 통한 상호작용에 대해서는 AGPL 13조가 적용되도록 정함으로써 그 범위 내에서 GPL 3.0이 적용되지 않음.

© 2016. Black Duck Software Korea all rights reserved.

오픈소스 라이선스 분류



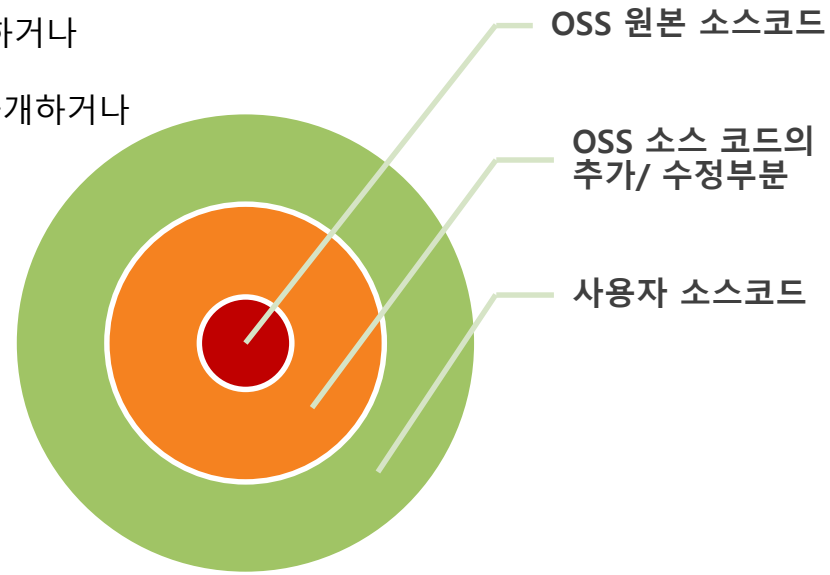
© 2016. Black Duck Software Korea all rights reserved.
BLACKDUCK

소스코드 공개범위

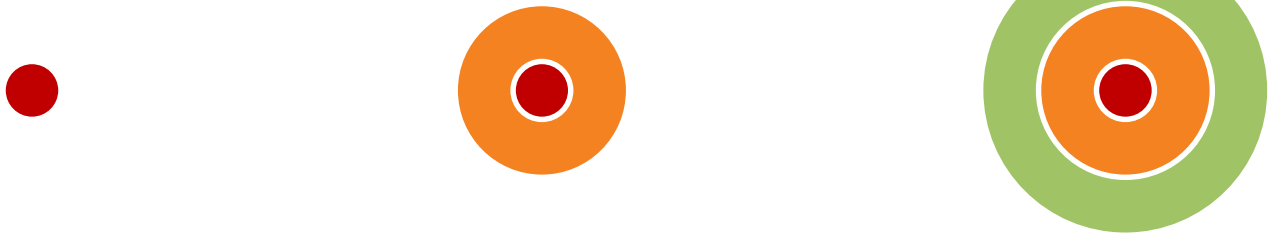
▣ Case 1. 경우에 따라 해당 오픈소스의 소스 코드만 공개 혹은 고지 하거나

▣ Case 2. 해당 오픈소스의 소스 코드를 수정 또는 추가한 부분까지 공개하거나

▣ Case 3. 해당 오픈소스와 링크된 모든 사용자 코드를 공개하거나



소스코드 공개 케이스



Case 1. OSS 원본 소스코드 공개

Case 2. OSS 원본 소스코드
+ 소스코드 추가 및 수정 부분 공개

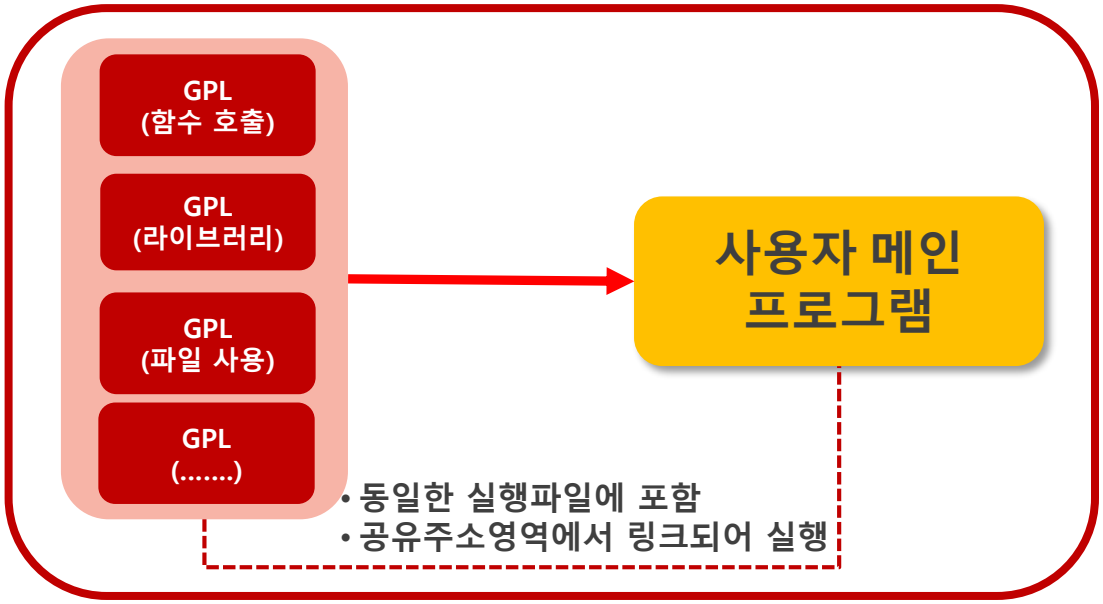
Case 3. OSS 원본 소스코드 +
소스코드 추가 및 수정 부분 +
OSS와 링크된 사용자 소스코드 공개

© 2016. Black Duck Software Korea all rights reserved.

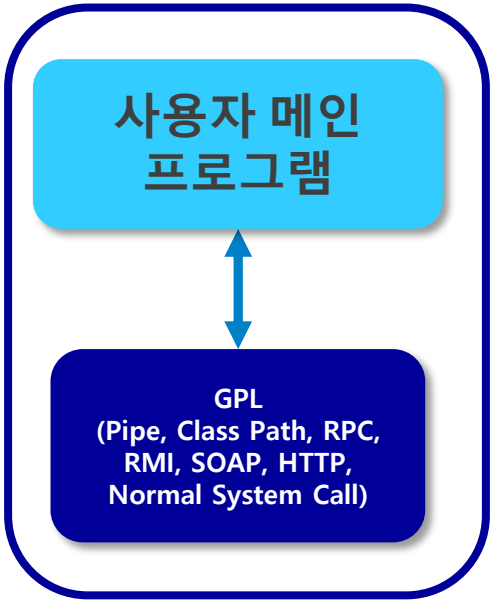
소스코드 공개범위(GPL)

▣ 수정한 내용에 대한 소스 공개 의무 발생, SW를 수정하거나 새로운 SW를 링크시키는 경우 하나의 프로세스로 동작하는 전체 프로그램의 소스 코드 공개 (동일한 실행 파일에 포함되는 경우, 공유주소영역(Shared address space) 에서 링크되어 실행되는 경우)

▣ 소스 코드 공개 예외상황
- 리눅스를 기반으로 개발된 Application, 커널 모듈 형태로 작성된 Loadable Device Driver 등에 의한 정상적인 리눅스 system call 을 사용하는 경우
- Class Path Exception 인 경우,
- 2개의 프로그램이 파이프(pipe), 소켓(socket), command line arguments 형태로 통신하는 경우



GPL과 동일조건으로 소스코드 공개



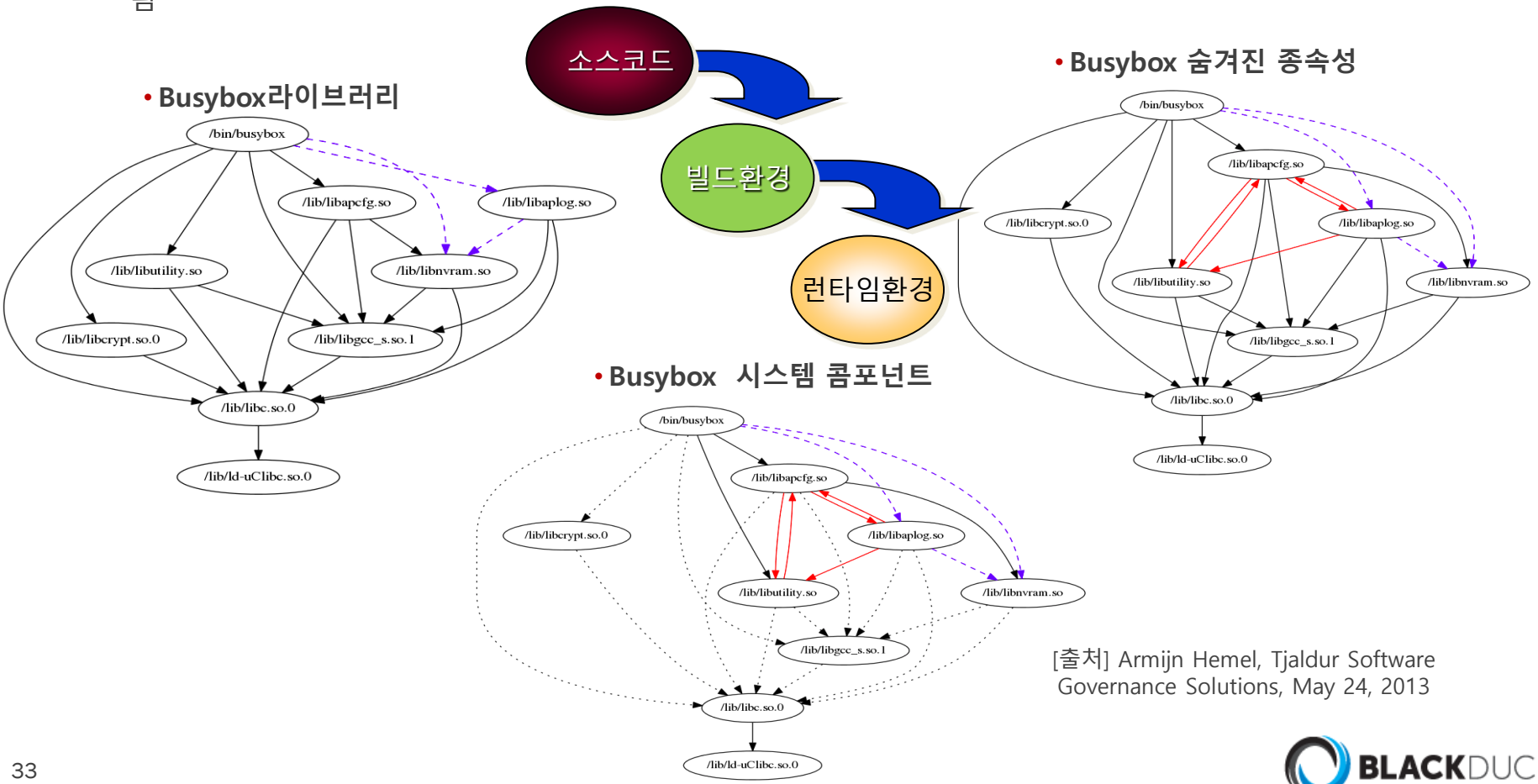
사용자 코드 비공개

© 2016. Black Duck Software Korea all rights reserved.

소스코드 공개범위(GPL)

▣ Executable and Linkable Format(ELF) 파일을 통한 파생저작물(Derivate Work)의 검토

- ELF는 리눅스 또는 다른 유닉스 시스템에서 가장 널리 사용되어지는 바이너리 형식
- 현재 Free Software Foundation에서는 모든 링킹 타입은 파생저작물을 생성한다고 주장하지만 많은 법률전문가들 사이에서 이견이 있음
- 공개된 소스코드는 콤포넌트 그 자체가 실행파일에 포함되지 않는다면, 실행파일을 구동하는 OS의 주된 콤포넌트들(컴파일로, 커널 등)과 정상적으로 배포되는 어떠한 것(소스 혹은 바이너리 형태)도 소스코드를 공개하지 않아도 됨



[출처] Armijn Hemel, Tjaldur Software Governance Solutions, May 24, 2013

BLACKDUCK

라이선스 양립성(Compatibility)

▣ 서로 다른 라이선스의 조합일 경우
  - 각각의 오픈소스 라이선스 의무사항이 서로 상충하여 양립할 수 없다면, 배포가 불가능 함

MPL 1.0(Mozilla public License)
다른 소스 코드와 결합하여 사용할 경우 수정된 MPL 파일을 반드시 MPL과 동일한 조건으로 공개

+

GPL 2.0(General public License)
다른 소스 코드와 결합하여 사용할 경우 결합하는 모든 소스 코드를 GPL과 동일한 조건으로 공개

=

mozilla FOUNDATION

FREE SOFTWARE FOUNDATION

MPL 2.0의 경우 secondary License를 GPL로 정의하여 GPL로 확대가능

© 2016. Black Duck Software Korea all rights reserved.
BLACKDUCK

라이선스 양립성(Compatibility)

▣ 개별 라이선스 들은 서로 다른 라이선스와 결합 사용함에 있어서 제약조건을 가지고 있음

라이선스	저작권자	최신버전	출시년도	다른 라이선스의 코드와의 링크	다른 라이선스로 인한 릴리즈 변경
Academic Free License	Lawrence E. Rosen	3	2002	Yes	Yes
Apache License	Apache Software Foundation	2.0	2004	Yes	Yes
Apple Public Source License	Apple Computer	2.0	August 6, 2003	Yes	No
Artistic License	Larry Wall	2.0	2000	Yes	With restrictions
Berkeley Database License	Oracle Corporation	?	February 7, 2008	No	No
BSD license	Regents of the University of California	?	?	Yes	Yes
Boost Software License	?	1.0	August 17, 2003	Yes	Yes
Common Development and Distribution License	Sun Microsystems	1.0	December 1, 2004	Yes	Yes
Common Public License	IBM	1.0	May 2001	Yes	No
Cryptix General License	Cryptix Foundation	?	1995	Yes	Yes
Eclipse Public License	Eclipse Foundation	1.0	?	Yes	No
Educational Community License	?	1.0	?	Yes	Yes
Eiffel Forum License	NICE	2	2002	Yes	Yes
IBM Public License	IBM	1.0	August 1999	Yes	Yes
GNU General Public License	Free Software Foundation	3.0	June 2007	No	No
GNU Lesser General Public License	Free Software Foundation	3.0	June 2007	Yes	No
Hacktivismo Enhanced-Source Software License Agreement	Hacktivismo/Cult of the Dead Cow	?	November 26, 2002	?	?
IBM Public License	IBM	1.0	August 1999	Yes	Yes

[출처] http://en.wikipedia.org/wiki/Comparison_of_free_software_licenses#General_comparison

© 2016. Black Duck Software Korea all rights reserved.

라이선스 양립성(Compatibility)

기타 라이선스와 GPL 양립성

라이선스 및 버전	GPL과의 양립성
Academic Free License	No
Apache License version 1	No
Apache License version 1.1	No
Apache License version 2	Yes
Apple Public Source License version 1.x	No
Apple Public Source License version 2.0	No
Artistic License 1.0	No
Clarified Artistic License (draft 2.0)	Yes
Artistic License 2.0	Yes
Berkeley Database License	Yes
original BSD license	No
modified BSD license	Yes
Boost Software License	Yes
Common Development and Distribution License	No
Common Public License	No
Creative Commons licenses (Tags: by & sa)	No
Creative Commons licenses (Tags: nc & nd)	No
Cryptix General License	Yes
Do What The Fuck You Want To Public License (WTFPL)	Yes
Eclipse Public License	No
Educational Community License	?
Eiffel Forum License version 2	Yes
GNU General Public License	Yes[3]
GNU Lesser General Public License	Yes

Apache version 2 is compatible to version 3 of the GPL
but not compatible to version 2.

© 2016. Black Duck Software Korea all rights reserved.

라이선스 양립성(Compatibility)

기타 라이선스와 GPL 양립성

라이선스 및 버전	GPL과의 양립성
Hacktivismo Enhanced-Source Software License Agreement	No
IBM Public License	No
Intel Open Source License	Yes
ISC license	Yes
LaTeX Project Public License	No
MIT license	Yes
Mozilla Public License	No
Netscape Public License	No
Open Software License	No
OpenSSL license	No
PHP License	No
POV-Ray-License	No
Python Software Foundation License 2.0.1; 2.1.1 and newer	Yes
Q Public License	No
Sun Industry Standards Source License	No
Sun Public License	No
Sybase Open Watcom Public License	?
W3C Software Notice and License	Yes
XFree86 1.1 License	Yes
zlib/libpng license	Yes
Zope Public License version 1.0	No
Zope Public License version 2.0	Yes

[출처] http://en.wikipedia.org/wiki/Comparison_of_free_software_licenses#General_comparison

© 2016. Black Duck Software Korea all rights reserved.

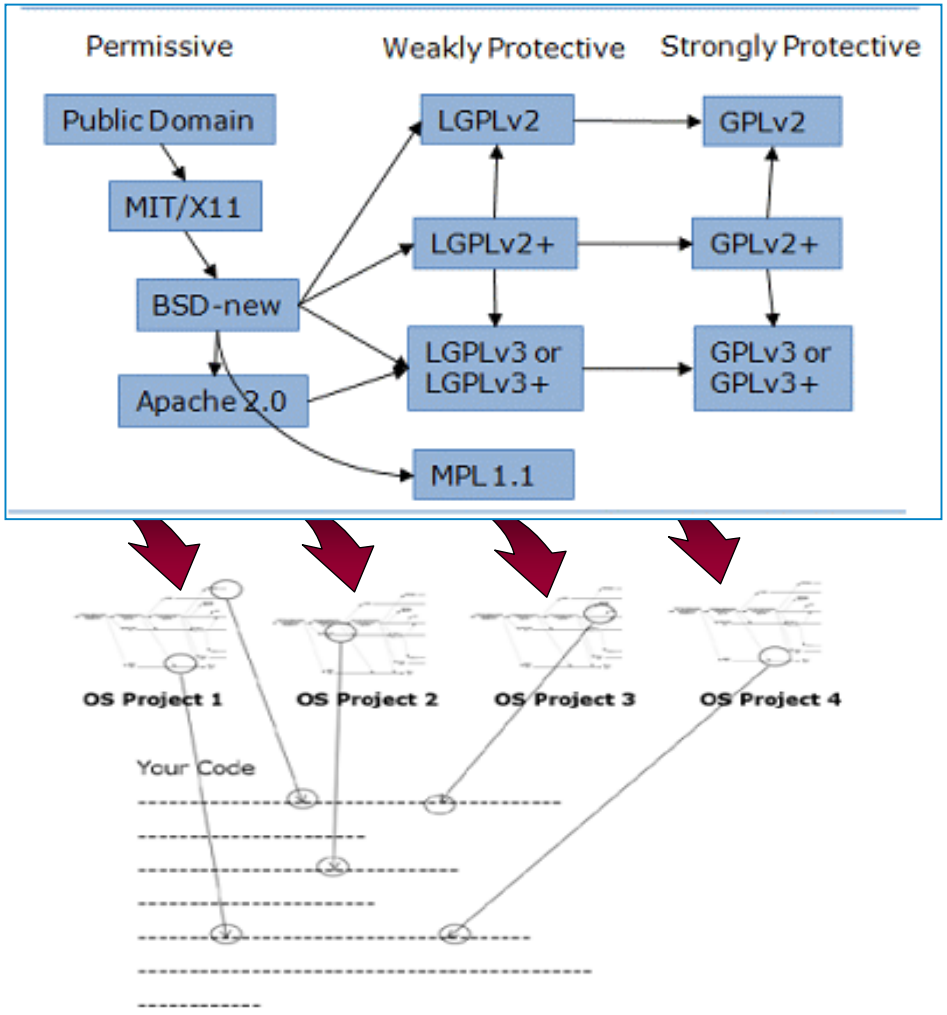
라이선스 의무사항 비교

No.	의무사항 \ 라이선스	Commercial License	GPL 2.0	GPL 3.0	LGPL 2.0	LGPL 3.0	GNU Affero General Public License 3.0	EPL 1.0	MPL 1.1	Apache 2.0	BSD 2.0
1	배포권리(오브젝트/바이너리코드 배포)	X	X	X	X	X	X	X	X	X	X
2	배포(소스코드배포에 의해서만 부여되는 의무사항)	X	◎	◎	◎	◎	◎	◎	◎	X	◎
3	소스코드배포/강제적 공유 의무사항	X	◎	◎	◎	◎	◎	X	◎	X	X
4	복제 권한 허용	X	◎	◎	◎	◎	◎	X	X	X	X
5	수정(개작)권한 허용	X	◎	◎	◎	◎	◎	X	X	X	X
6	역설계 권한 허용	X	◎	◎	◎	◎	◎	X	X	X	X
7	차별적 제한 금지 ◎ or 차별적 제한 있음 ●	X	◎	◎	◎	◎	◎	◎	◎	●	X
8	추가 복제에 대한 로열티 및 수수료 금지	X	◎	◎	◎	◎	◎	◎	◎	X	X
9	특허보복(특허소송 제기시 라이선스 종료)	X	X	◎	X	◎	◎	◎	◎	◎	X
10	명시적 특허라이선스(특허소송을 제기하지 않음)	X	X	◎	X	◎	◎	◎	◎	X	X
11	DRM금지	X	X	◎	X	◎	◎	X	X	X	X
12	고지(특정법률 혹은 속성)	X	◎	X	◎	◎	◎	X	X	X	X
13	변경사항 고지	X	◎	◎	◎	◎	◎	◎	◎	◎	X
14	변경사항에 대해 원저작자에게 사용허가	X	X	◎	X	◎	◎	◎	◎	X	X
15	다른사람을 대신한 보증의 부인	◎	◎	X	◎	X	X	◎	◎	◎	X
16	다른사람의 책임의 제한	◎	◎	X	◎	X	X	◎	◎	◎	X
17	배포/사용으로 인해 발생한 원저작자의 클레임에 대한 배상	X	X	X	X	X	X	◎	◎	◎	X
18	배포시 라이선스 사본 포함	X	◎	◎	◎	◎	◎	◎	◎	◎	◎
19	광고/홍보시 배포자,저작자, 특정상표사용 금지	X	X	X	X	X	X	X	◎	◎	◎
20	원코드와 동일조건 허가	X	◎	◎	◎	◎	◎	◎	◎	X	X
21	라이선스 확장 범위(공개범위)	X	코드 기반의 산출물 (per GPL)	코드 기반의 산출물 (per GPL)	동적라이브러리(per LGPL)	동적라이브러리(per LGPL)	코드 기반의 산출물 (per GPL)	모듈 (per EPL/CPL)	파일 (per MPL)	X	X

© 2016. Black Duck Software Korea all rights reserved.

오픈소스 라이선스 생태계

- 오픈소스 라이선스는 라이선스의 조건에 따라 파생물의 재 배포 시에 원 라이선스와 동일조건으로 배포해야 하는 라이선스(GPL, LGPL, MPL 등)와 원 라이선스와 관계없이 다른 라이선스로 변경 재배포가 가능한 라이선스(BSD, MIT, Apache 등)가 있음.



© 2016. Black Duck Software Korea all rights reserved.

애플/구글 앱스토어의 오픈소스 현황

2010년 OpenLogic 분석자료

	iPhone/iPad Apps	Android Apps
Apps Analyzed	364 top apps from iTunes Store	90 top apps from Android Marketplace
% with OSS	41% of apps (149)	88% of apps (79)
% with GPL	8% of apps (30)	3% of apps (2)

2011년 안드로이드 개발자 컨퍼런스 OpenLogic 분석자료

- 분석대상앱
  - 카테고리별 가장 많이 사용되는 유료와 무료 앱을 각 10개씩
  - TV에 광고되는 앱
  - 포춘 500대 기업 중 25위 안의 기업들이 발표한 앱
- 분석대상 앱수: 애플 523개, 안드로이드 112개, 총 635개
- 분석대상 앱중 52개 앱 아파치 라이선스 활용, 16개 앱이 GPL 혹 LGPL 활용
- **오픈소스를 활용한 앱 중 71%가 의무사항 위반**
- 일부 오픈소스 앱의 경우 자체 사용자 약관을 적용하여 앱에 대한 저작권 주장
- 2012년 다시 오픈소스 활용한 동일한 앱 66개를 분석: **38.3% 오픈소스 라이선스 위반**
- 오픈소스 준법성 미비로 인해 서비스가 중지될 경우 심각한 경제적 파장 초래 가능

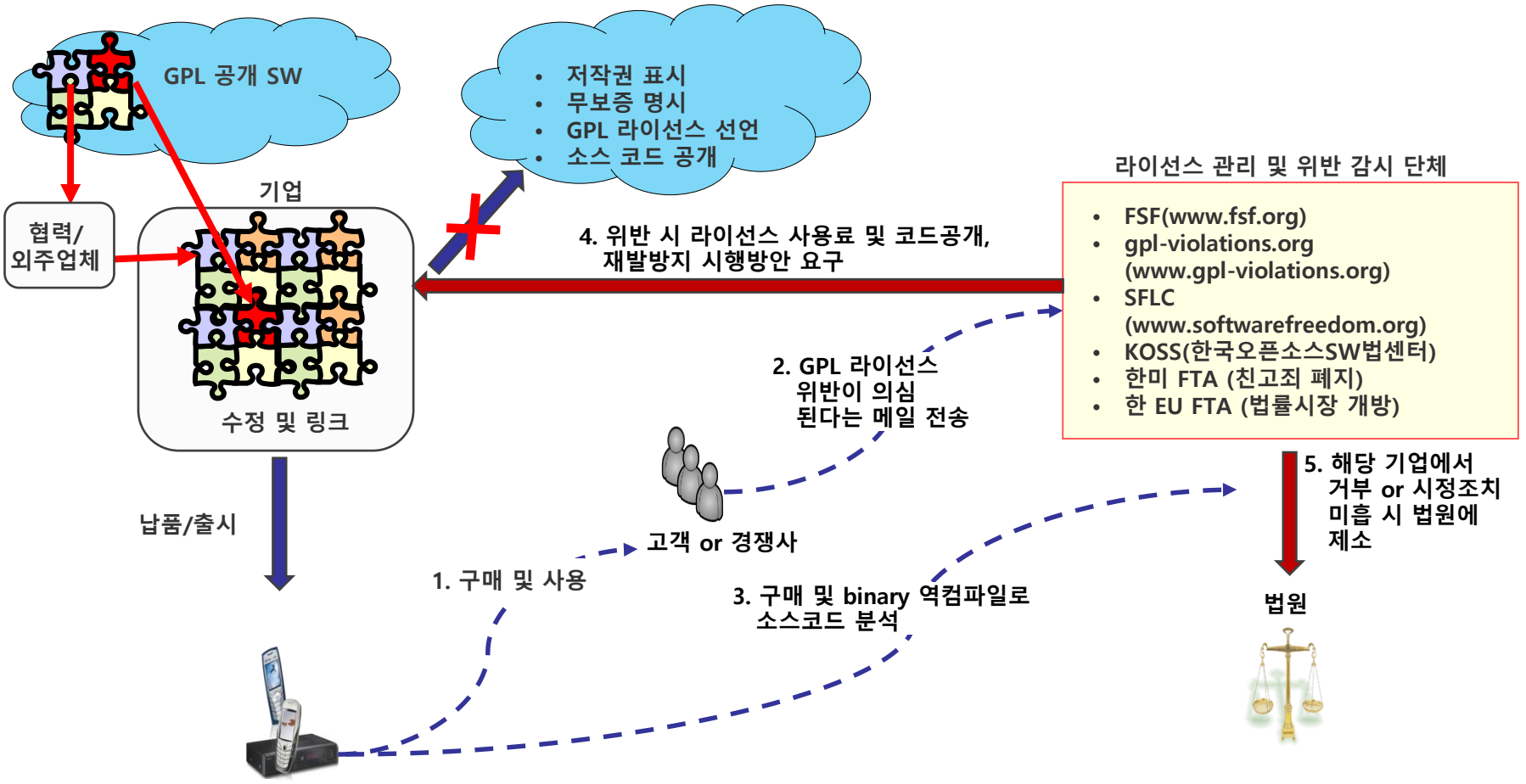
© 2016. Black Duck Software Korea all rights reserved.

3. OSS 라이선스 관리와 위반사례

© 2016. Black Duck Software Korea all rights reserved.

BLACKDUCK

오픈소스 라이선스 위반 모니터링



© 2016. Black Duck Software Korea all rights reserved.

오픈소스 라이선스 위반시 법적 효과

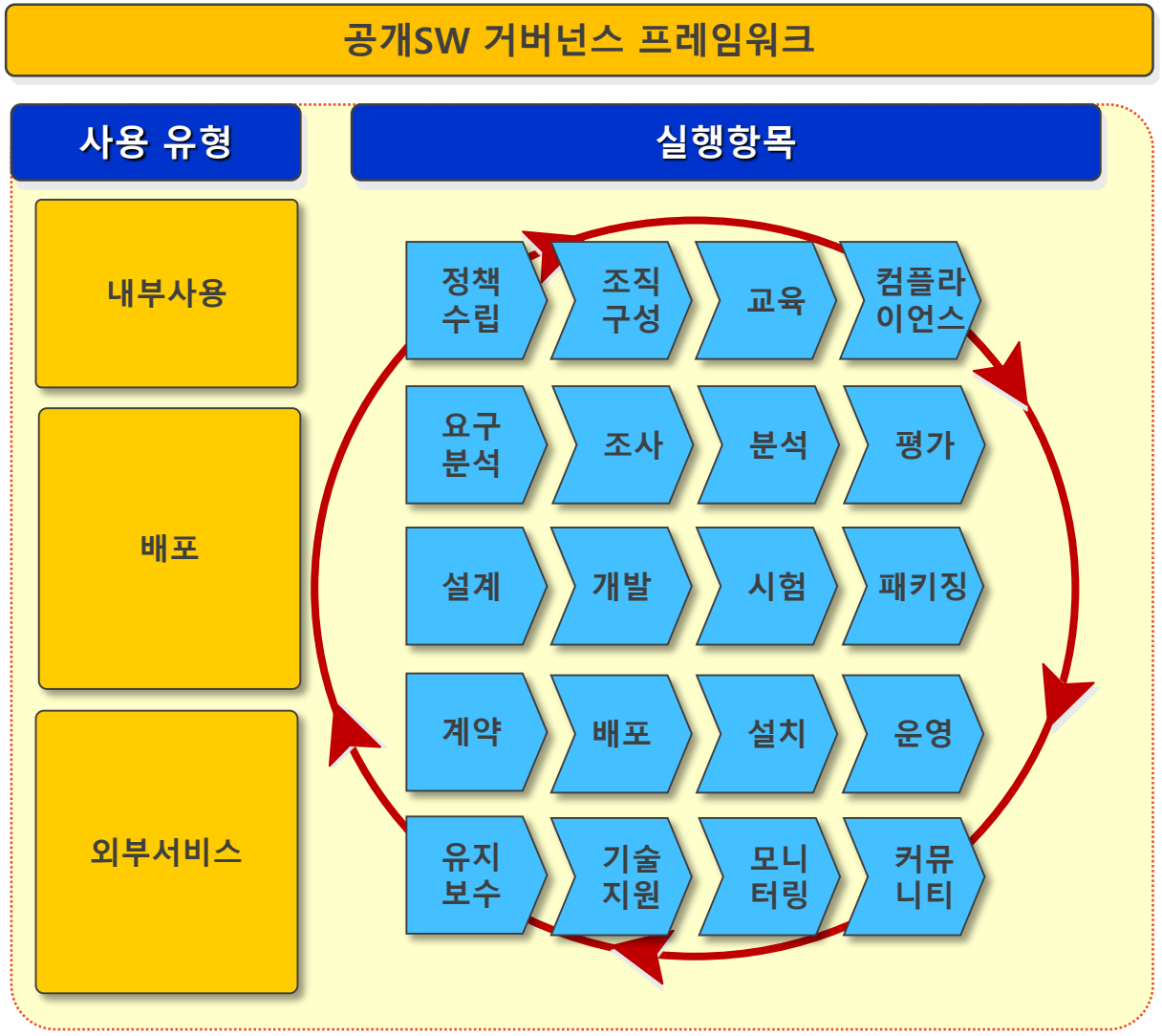
▣ 오픈소스 라이선스를 위반하게 되면 민사상 손해배상, 형사고소와 조직에 있어서의 다양한 손해를 야기시킴

민사상 손해배상	• 저작권침해금지 가처분: 보전의 필요성 소명
기타 손해	• 기업평판, 서비스 정지, 대체비용 등
형사고소	• FTA 이후 부분적 비 친고죄화 ▪ 영리목적 OR 상습적 • 양벌 규정 ▪ 행위자를 처벌하는 외에 그 행위자를 사용하는 법인의 대표자나 법인도 처벌 가능 • 위반행위를 방지하기 위해 상당한 주의와 감독을 하였음을 입증

[출처] 한국오픈소스SW법센터

© 2016. Black Duck Software Korea all rights reserved.

오픈소스 라이선스 거버넌스



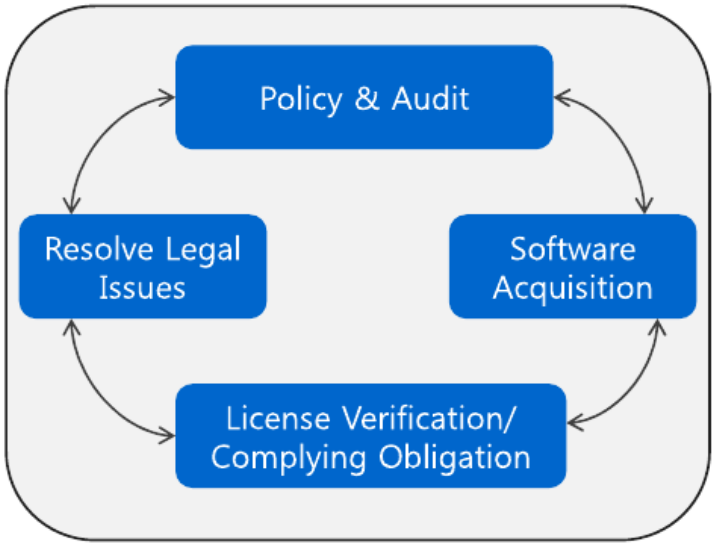
[출처] 공개W역량프라자

© 2016. Black Duck Software Korea all rights reserved.

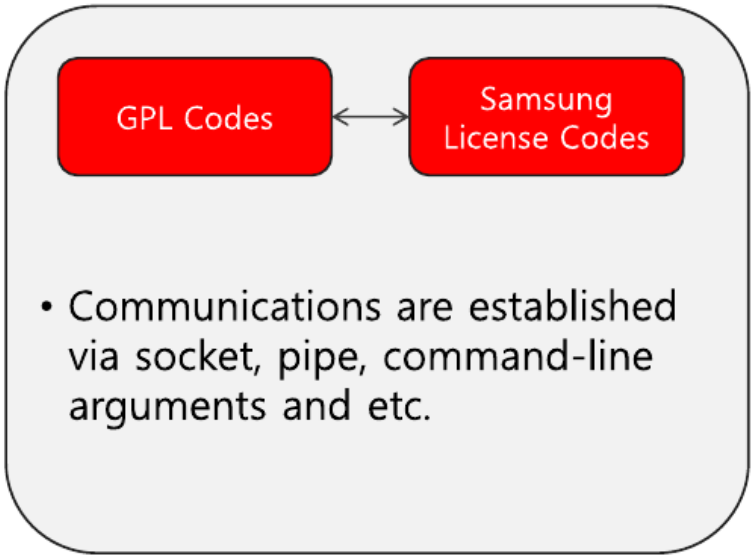
삼성전자 오픈소스 거버넌스

- Samsung respects open source communities and fulfils the license of sources
- Samsung has several preparations to use open sources legally

- **OSAB (Open Source Advisory Board)**
  - Samsung operates 4 different organizations to verify the legality of sources



- **Violation Prevention (Design Separation)**
  - Samsung aims an independent modular SW design
  - This prevents a license violation case on the off chance

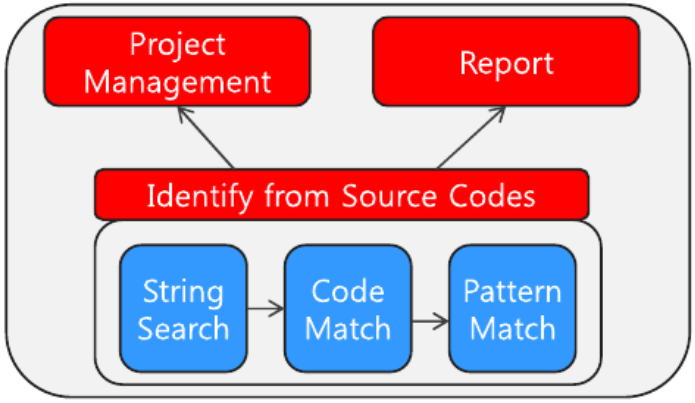


[출처] 삼성전자 http://events.linuxfoundation.org/images/stories/pdf/klf2012_park.pdf

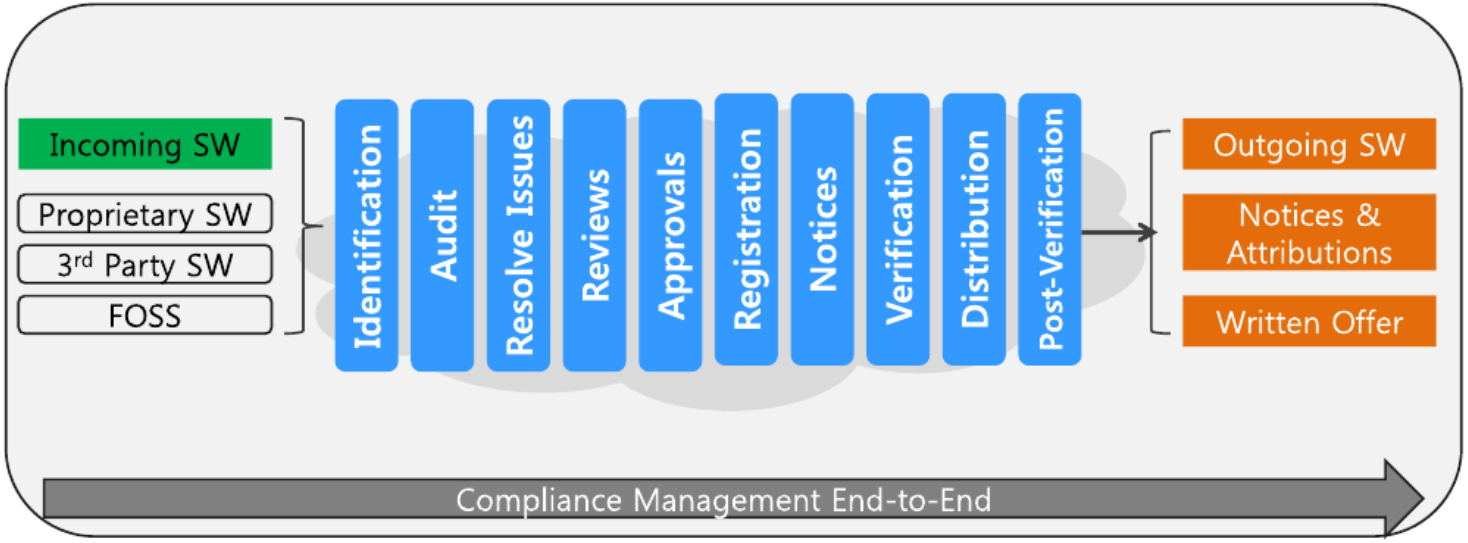
© 2016. Black Duck Software Korea all rights reserved.
BLACKDUCK

삼성전자 오픈소스 거버넌스

- **License Verification Process**
  - When the code design is finished, Samsung proceeds a verification for the license legality
  - Samsung utilizes professional tools such as Protex and OSI Tools



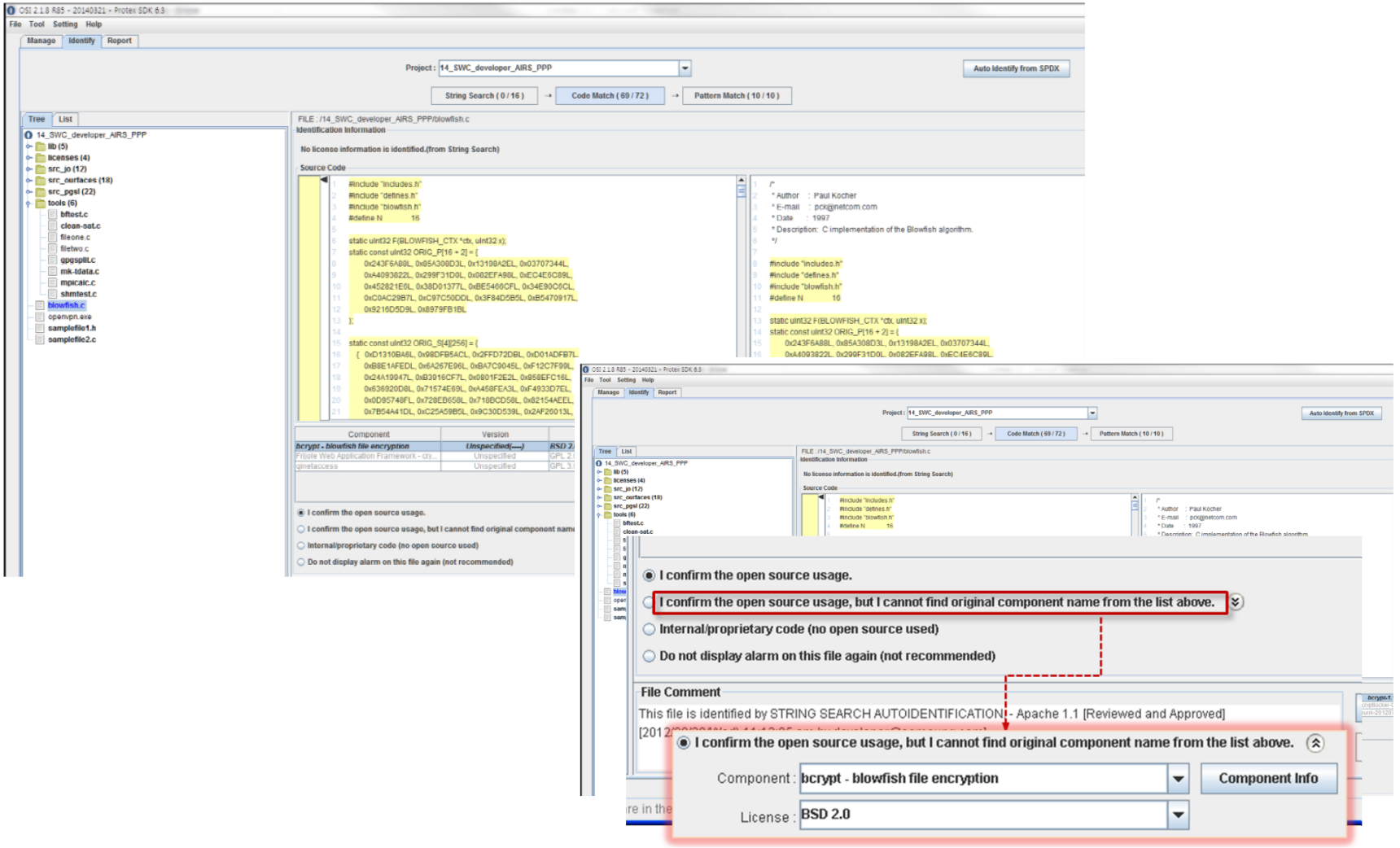
- **End-to-End Compliance Management**



[출처] 삼성전자 http://events.linuxfoundation.org/images/stories/pdf/klf2012_park.pdf

© 2016. Black Duck Software Korea all rights reserved.

삼성전자 자주검증 도구(OSIT)

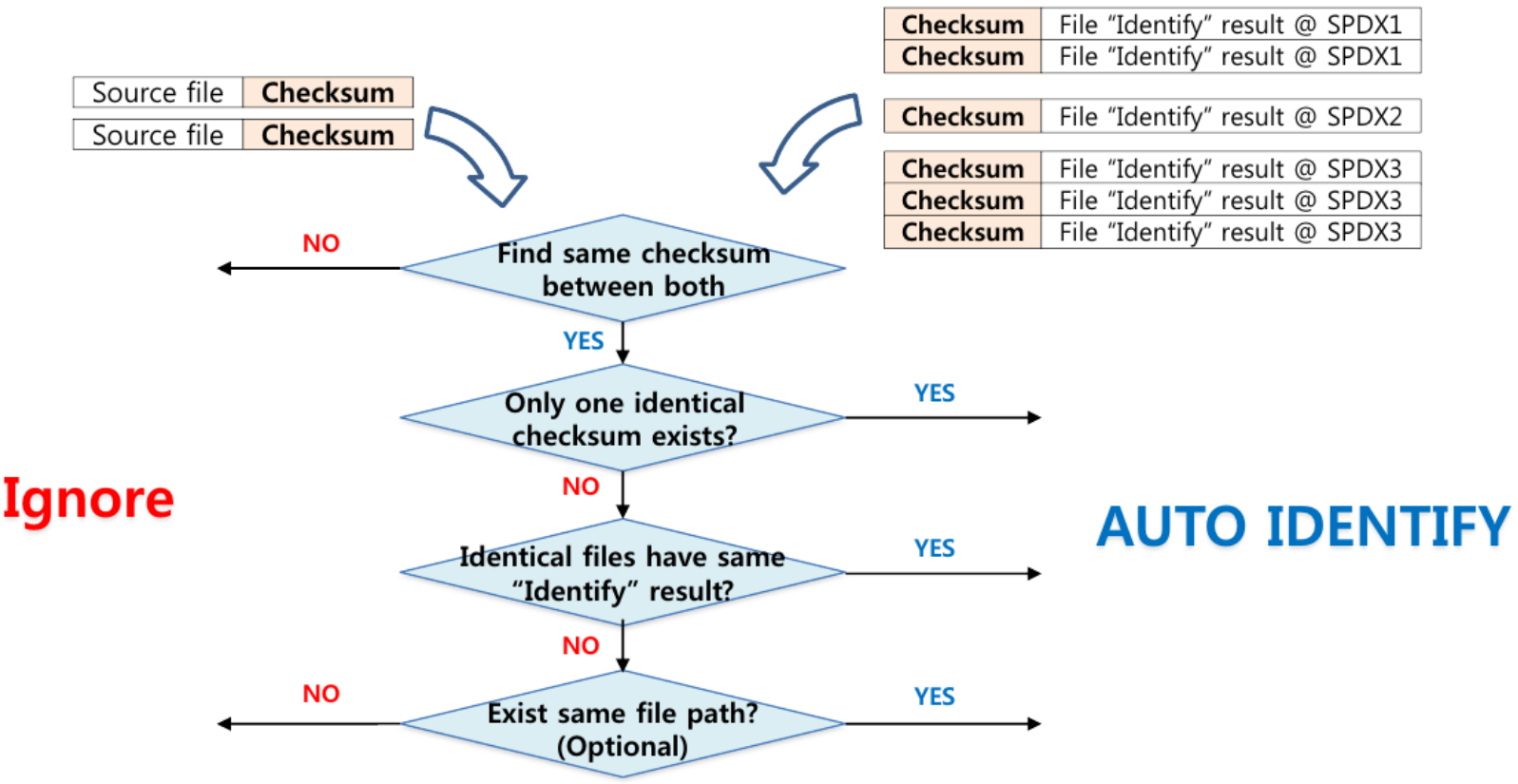


[출처] 삼성전자 2014 삼성 오픈소스 컨퍼런스 발표자료 : Introduction to SPDX for Better Compliance

© 2016. Black Duck Software Korea all rights reserved.

삼성전자(SPDX를 활용한 공급망 관리)

- **AIRS** (**A**uto **I**dentifie**R** using **S**PDX)
  - Import "Identify" result from multiple SPDX files.



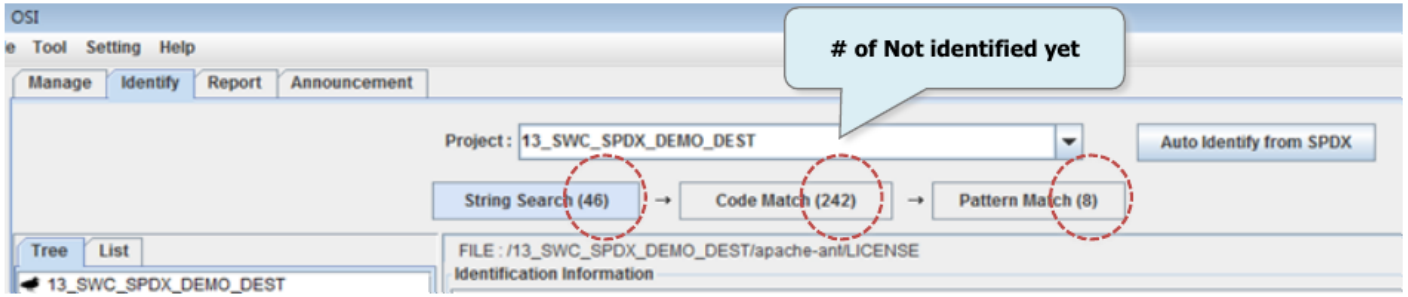
[출처] 삼성전자 2014 삼성 오픈소스 컨퍼런스 발표자료 : Introduction to SPDX for Better Compliance

© 2016. Black Duck Software Korea all rights reserved.

삼성전자(SPDX를 활용한 공급망 관리)

- **AIRS** (Auto IdentifieR using SPDX)

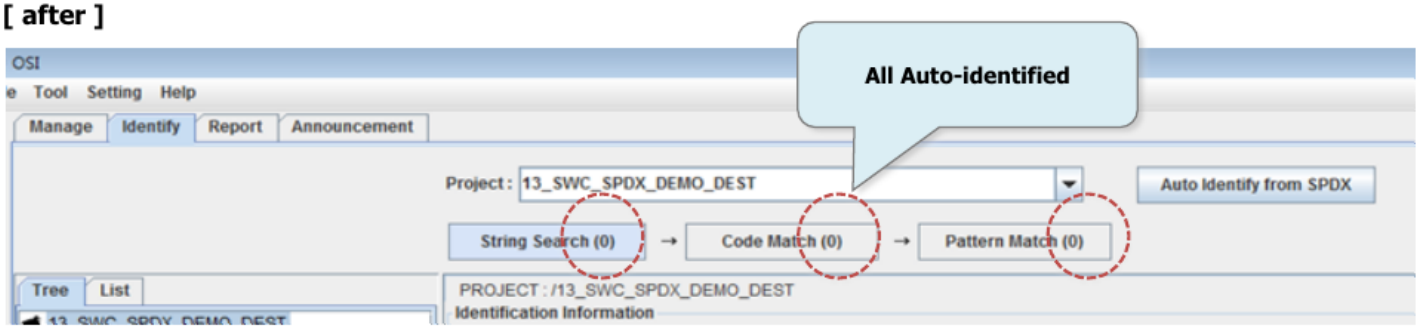
[before]



Execute AIRS

ex)
java –jar airs.jar **ai –h** http://127.0.0.1 **–u** developer@samsung.com **–p** passwd –proxy-host 127.0.0.1 --proxy-port 8080
--project-id c_13_swc_developer_ai_demo_130826 **--spdx-files** source.rdf

[after]



※ OSI: Open source Self Inspector (samsung in-house tool)

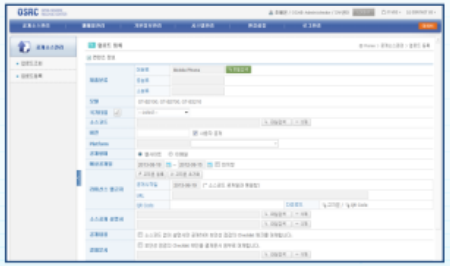
[출처] 삼성전자 2014 삼성 오픈소스 컨퍼런스 발표자료 : Introduction to SPDX for Better Compliance

© 2016. Black Duck Software Korea all rights reserved.

삼성전자(오픈소스 배포 프로세스)

[Generating Open Source License Notice using SPDX] – Easy to generate

Uploading Source code



Admin page in opensource.samsung.com

Load Verification Result(SPDX)

License Notice and QR Code(URL) created

[Providing QR Code instead of full acknowdgement] – Easy to Change

QR Code/URL included as part of the product documentation (in manual, on box, in device with written offer, etc.)

Ex) QRCode on box

End user visits specified Web site(OSRC) using QR Code (or connect to URL directly)

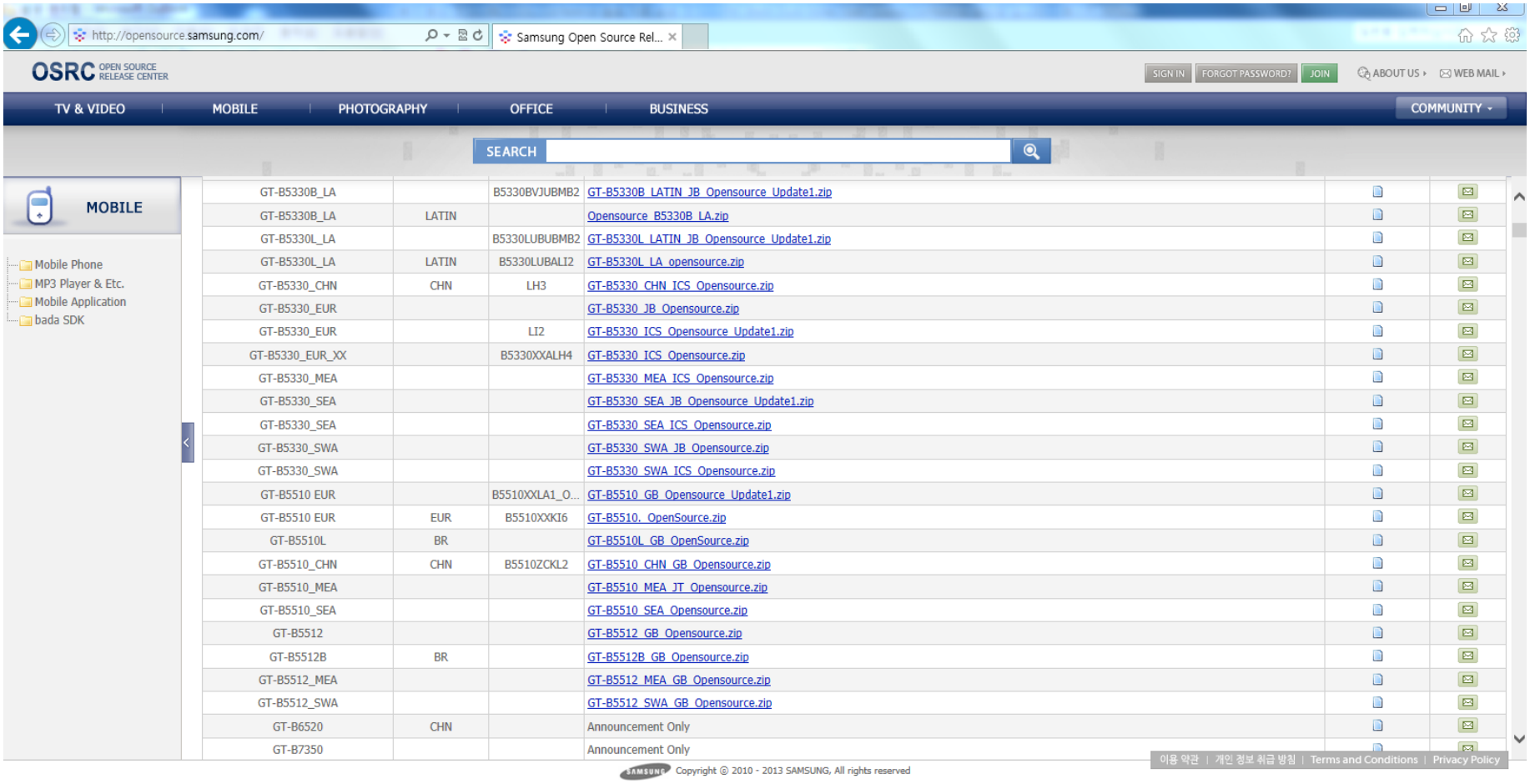
End user receives license info in the product including source code, license, and compliance contact

[출처] 삼성전자 2014 삼성 오픈소스 컨퍼런스 발표자료 : Introduction to SPDX for Better Compliance

© 2016. Black Duck Software Korea all rights reserved.

Use Case (코드공개)

▣ 삼성전자에서는 오픈소스 코드 공개 및 고지 의무사항을 준수하기 위해 OSRC(Open Source Release Center)를 운영하고 있음



[출처] http://opensource.samsung.com/reception.do

© 2016. Black Duck Software Korea all rights reserved.

Use Case (라이선스 사용 고지)

▣ 삼성전자에서는 Apache License Version 2.0과 같이 코드 공개 의무사항이 없지만 사용자 고지 의무사항을 준수하기 위해 Open Source Announcement를 고지하고 있음

Open Source Announcement

Some software components of this product incorporate source code covered under the BSD and Australian Public License B (OZPLB).

And this product includes software developed by the NetBSD Foundation, Inc. and its contributors.

Component	License
Windows Template Library	Microsoft Permissive License (Ms-PL)
Khronos Group - OpenGL ES 1.X	SGI Free Software License B 1.0
Android Open Source Project	Apache License Version 2.0
Code Project	Code Project Open 1.02 License
Common L4	Australian Public Licence B (OZPLB) Version 1-0
Copyright (c) Regents of the University of California	Regents of University of California License
Copyright (c) Carnegie Mellon University	CarnMellon Mach OS License
NetBSD	BSD 1.0

Microsoft Permissive License (Ms-PL)

Published: October 18, 2005

This license governs use of the accompanying software. If you use the software, you accept this license. If you do not accept the license, do not use the software.

1. Definitions
   * The terms "reproduce," "reproduction" and "distribution" have the same meaning here as under U.S. copyright law.
   * "You" means the licensee of the software.
   * "Licensed patents" means any Microsoft patent claims which read directly on the software as distributed by Microsoft unde this license.
2. Grant of Rights
   1. Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, Microsoft grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce the software, prepare derivative works of the software

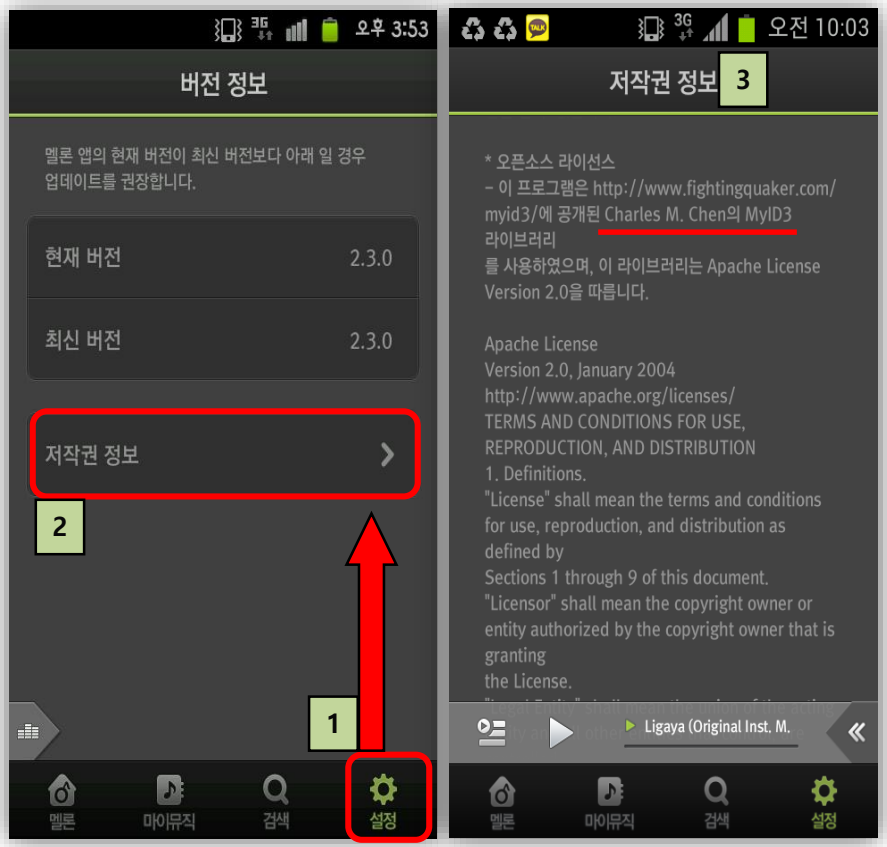
[출처] http://opensource.samsung.com/reception.do

© 2016. Black Duck Software Korea all rights reserved.

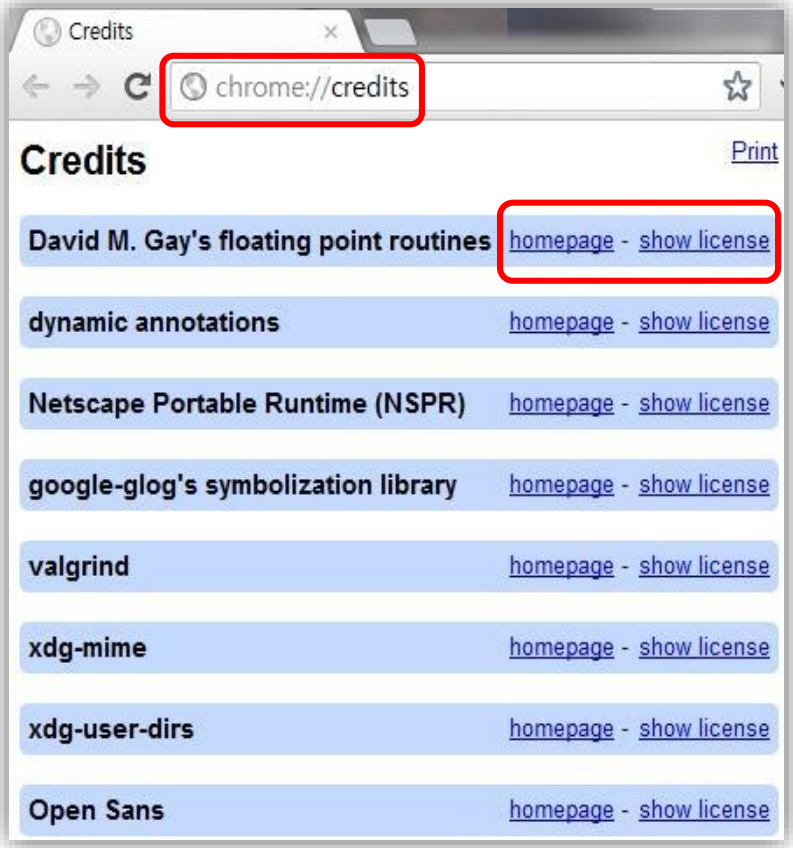
Use Case (라이선스 사용 고지)

▣ SK 플래닛의 라이선스 사용 고지

Text 고지 방식



홈페이지 링크 방식



Check Point : Server-side 고지 or App 내 고지

[출처] SK플래닛

© 2016. Black Duck Software Korea all rights reserved.

Use Case (코드 공개 및 라이선스 사용 고지)

▣ 벤츠, GM, 아우디 등 글로벌 자동차업체에서도 관련 오픈소스에 대한 코드공개 혹은 고지 의무를 수행하고 있음

GM

GM

Open Source Downloads

volt, ampera, sail, and spark bev

Welcome to the Volt / Ampera, Sail, and Spark BEV Open Source Downloads Website!

Select Model Year

Make	Model	Year	
Chevrolet	Volt	2011	Select
Chevrolet / Opel, Vauxhall	Volt / Ampera	2012	Select
Chevrolet, Holden / Opel, Vauxhall	Volt / Ampera	2013	Select
Chevrolet	Spark BEV	2014	Select
Sail	SPRINGO EV	2014	Select

[출처] http://www.oss.gm.com

Chevy Volt User Manual

Open Source Information

This vehicle contains open source software, including without limitation, software distributed and/or modified under the GNU General Public License, Version 2, June 1991, and the GNU Lesser General Public License, Version 2.1, February 1999.

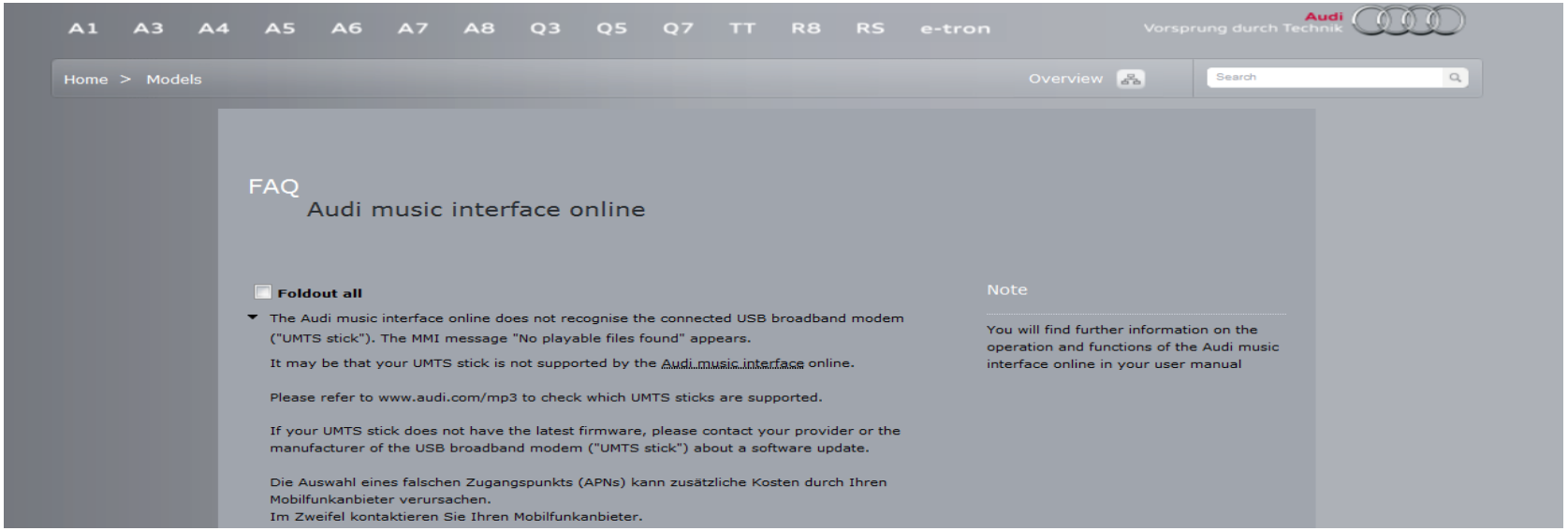
See www.oss.gm.com for additional information and to download related materials, including without limitation, the previous referred to licenses and software.

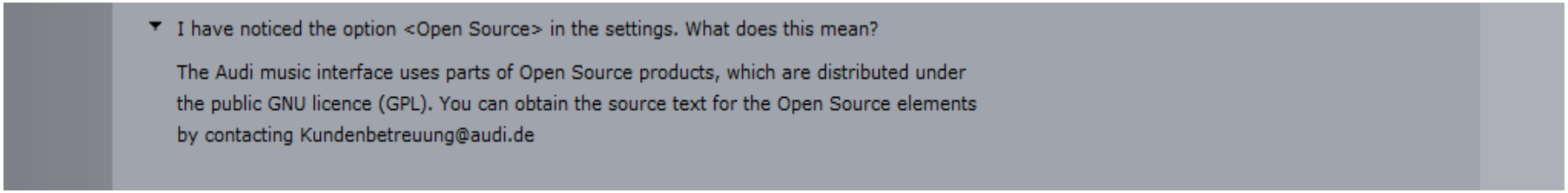
© 2016. Black Duck Software Korea all rights reserved.

Use Case (코드 공개 및 라이선스 사용 고지)

▣ 벤츠, GM, 아우디 등 글로벌 자동차업체에서도 관련 오픈소스에 대한 코드공개 혹은 고지 의무를 수행하고 있음

Audi





[출처] http://www.audi.com/com/brand/en/models/infotainment_and_communication/audi_music_interface_online/faq.html

© 2016. Black Duck Software Korea all rights reserved.

SAP 오픈소스 거버넌스 프로세스

Open source request form → Architecture Check → Legal &IP Evaluation → Applicant Briefing → Management Approval

General License Evaluation

- Warranties / liabilities
- Support offerings
- General license grant
- Export restrictions

Modifications

- Does the license allow for modifications?
- What terms apply to modifications?

Special Requirements

- Required text for documentation
- Copyright notices
- Distribution pre-requisites in general

IP Evaluation

- Product's characteristics
- Contribution policy
- Companies supporting and using the open source product

© 2016. Black Duck Software Korea all rights reserved.

블랙덕 오픈소스 성숙도 모델

	Exposed	Measured	Managing	Participating	Driving
Discovery	• No formal guidelines or processes	• Some guidelines provided	• Clear policy on acceptable sources and attributes; • Developers educated	+Tools to facilitate search and verification of attributes	+Participation in key communities to drive company's requirements
Review and Selection	• ad hoc	• Incorporated components are identified and tracked	• Clear policy and process; • Oversight and exception handling by review board	+Automated process insuring compliance	+Active involvement with key communities creates responsive FOSS supplier relationships
Code Management	• FOSS included and managed with proprietary code	• FOSS is tracked separately	• Policy establishes owner and responsibilities for each component; • FOSS repository; • Use tracking	+Automated process tracks sources, attributes, use and compliance requirements	+FOSS repository extended to support external releases
Maintenance and Support	• ad hoc	• Some approach to stay abreast of bug fixes and new releases	• Policy defines responsibilities for each component owner; • Consolidated support model	+Automated process tracks issues, fixes, versions	+Support model extended externally; +Automated process extended to handle external support
Compliance Program	• ad hoc, if any	• Incorporated FOSS components listed for each release; • Compliance requirements assembled by hand	• Review and code management processes prevent surprises; • Automated audit of product releases; • Compliance process with reporting	+Automated process integrates review, code management and compliance functions; +Automated reporting for management and customers	+Policy and automated process for audit and review of contributions
Community Interaction	• Download code	• Download code	• Download code; • Track updates; • Participate in forums *without* company identification	+Participate in forums *with* company attribution; +Contribute bug fixes	+Contribute new projects/components; +Sponsor key communities
Executive Oversight	• Probably none	• Executives receive lists of FOSS components in use	• Legal & line-of-business management participation on review board	+Policy for community participation; +Process for contribution of bug fixes	+Policy and process for contributing components, sponsorship for projects

© 2016. Black Duck Software Korea all rights reserved.
BLACKDUCK

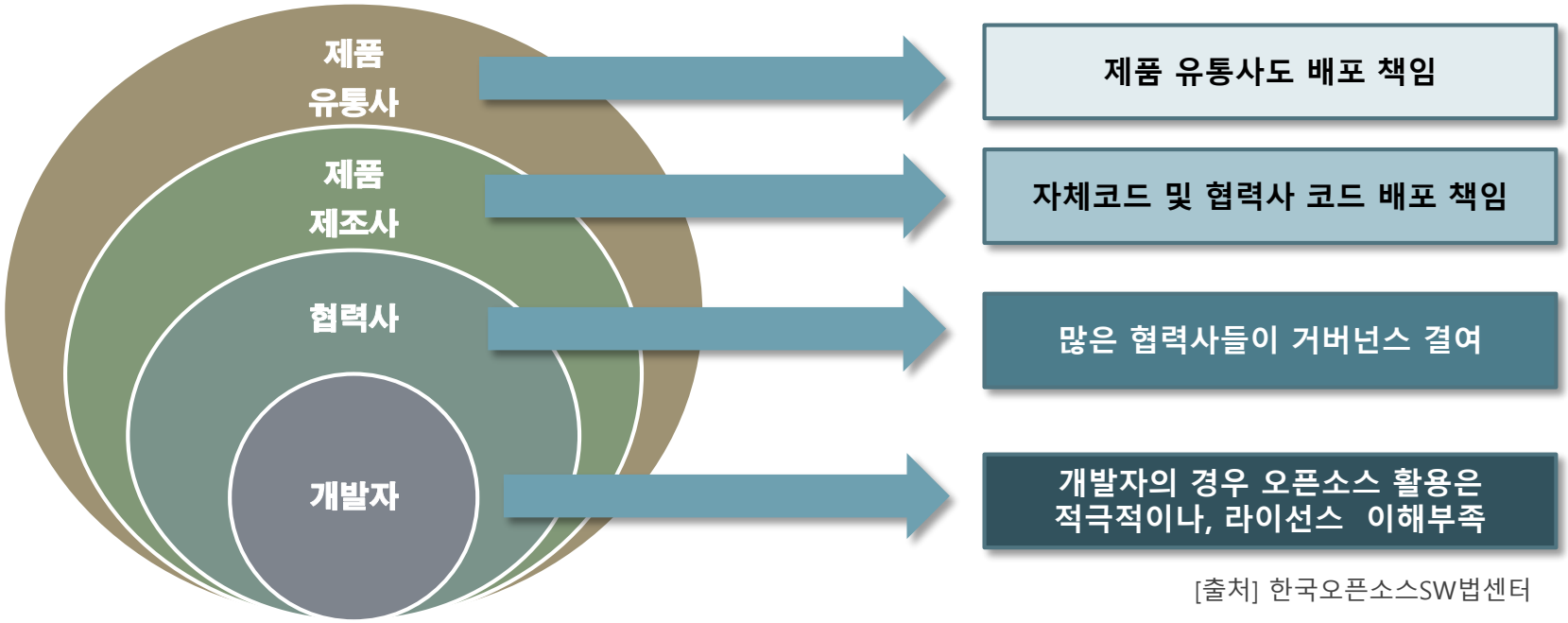
오픈소스 공급망 관리

▣ 배포

- 대부분의 오픈소스 소프트웨어의 경우 배포 시 의무 발생
- 배포하지 않을 경우 자유로운 수정, 사용의 권리가 있음
- AGPL의 경우 배포없이 온라인 등으로 서비스를 할 경우에도 소스코드 공개의무 등 발생

▣ 배포자의 관점

- 최종 소비자 입장 : 오픈소스 소프트웨어가 포함된 제품 제작사
- 라이선스 저작권자 입장 : 오픈소스 소프트웨어의 공급 망에 있는 모든 관계사(오픈소스 활용한 개발사, 오픈소스 활용 부품 공급자. 오픈소스 활용 완제품 생산자, 오픈소스 활용 제품 판매사)



[출처] 한국오픈소스SW법센터

© 2016. Black Duck Software Korea all rights reserved.

오픈소스 공급망 관리

▣ 협력사 오픈소스 거버넌스 검토

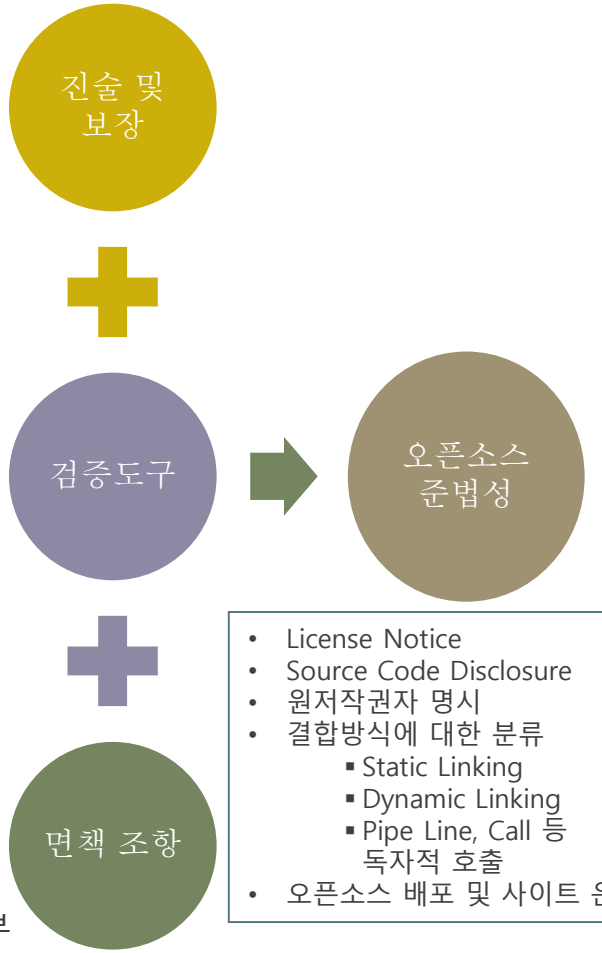
- 사용중인 오픈소스의 현황을 파악하는 Identification 단계
- Audit 및 라이선스 충돌 문제 해결 및 검사 보고서 작성 단계
- 설계분석(Architecture Review)과 연동분석(Link Analysis Review)
- 오픈소스 사용 승인 단계
- 오픈소스 컴포넌트 별 등록 단계
- 오픈소스 저작권 통지 및 배포 전 검증 단계
- 배포 및 최종 검증단계로 구분

▣ 협력사 거버넌스 검토대상

- 오픈소스 거버넌스 정책 수립 여부 및 검토
- 오픈소스 준법성 검증도구의 사용 여부
- 오픈소스 준법성 책임자의 역할 및 존재 여부
- 오픈소스 준법성 관련 라이선스 고지, 공개 여부
- 오픈소스 준법성 관련 임직원 교육 여부
- 오픈소스 준법성 관련 매뉴얼 및 체크리스트 작성 여부
- 오픈소스 라이선스 선별 정책의 존재 여부 및 자사 프로젝트와 양립성 여부

▣ 협력사 오픈소스 정책 세부내용

- 거버넌스 구축 및 소스코드 현황 분석 여부확인
- 라이선스 선별정책의 확인 및 발주사 선별정책과 상충 검토여부
- 개발된 제품에 대한 라이선스 검증 여부
- 최종결과물에 대한 소프트웨어 구성요소 확인 및 결합방식에 대한 분석 여부
- 해당 프로젝트에 적용되는 Use Case에 따른 의무사항 준수여부



[출처] 한국오픈소스SW법센터

© 2016. Black Duck Software Korea all rights reserved.

오픈소스 라이선스 검증 보고서

▣ 프로젝트 개요

프로젝트 라이선스	**Basic Proprietary Commercial License(상용 라이선스)**
분석 파일 수	**100Files**
분석된 바이트 수	**100MB**
OSS사용 파일 수	**50(50%)**

▣ 프로젝트 구성요소 목록(Bill of Materials)

준법성 현황	콤포넌트	버전	홈페이지	라이선스	결합형태	해당파일 수
다른 컴포넌트 라이선스와 충돌	Apache Lucene Java	1.4.3	http://jakarta.apache.org/lucene/docs/index.html	Apache License Version 2.0	Component	1
충돌없음	db-charmer	Unspecified	http://github.com/kovyrin/db-charmer/	MIT License V2	File	25
프로젝트에 선언된 라이선스와 충돌	GnuPG	Unspecified	http://www.gnupg.org/	GPL 3.0	File	6
N/A	optical_catalyst	Unspecified		Basic Proprietary Commercial License	Original Code	147
프로젝트에 선언된 라이선스와 충돌	petris	Unspecified	http://github.com/gitpan/petris/	GPL 2.0	File	16
충돌없음	PostgreSQL Database Server	Unspecified	http://www.postgresql.org/	PostgreSQL License	File	23

© 2016. Black Duck Software Korea all rights reserved.

오픈소스 라이선스 검증 보고서

▣ 오픈소스 라이선스 종합요약

라이선스	결합형태	해당파일수	%
Apache License Version 2.0	Component	26	5.20%
MIT License V2	File	25	5.00%
GPL 3.0	File	116	23.20%
GPL 2.0	File	24	4.80%
Sun Code Sample License	File	20	4.00%
OpenSSL Combined License	File	118	23.60%
PostgreSQL License	File	23	4.60%
[template] Basic Proprietary Commercial License	Original	148	29.60%
합계		500	100%

© 2016. Black Duck Software Korea all rights reserved.

오픈소스 라이선스 검증 보고서

▣ 검증분석 종합의견

검증분석 종합의견			
프로젝트 라이선스	Basic Proprietary Commercial License		
직접충돌 라이선스	수정권리를 부여하지 않는다.	GPL 2.0	수정권리를 부여하는 것이 필요하다. (per GPL).
	소스코드를 배포하지 않는다.		소스코드 배포가 필요하다. (per GPL).
	코드 사용에 대해 수수료를 부과한다.		코드를 사용함에 있어 관련된 수수료를 부가할 자격이 없다.
	리버스엔지니어 권리를 부여하지 않는다.		리버스엔지니어 권리를 부여하는 것이 필요하다. (per GPL).
	복제에 대한 권리를 부여하지 않는다.		복제에 대한 권리를 부여하는 것이 필요하다. (per GPL).
	수정권리를 부여하지 않는다.	GPL 3.0	수정권리를 부여하는 것이 필요하다. (per GPL).
	소스코드를 배포하지 않는다.		소스코드 배포(네트웍서비스 포함)가 필요하다. (per GPL).
	코드 사용에 대해 수수료를 부과한다.		코드를 사용함에 있어 관련된 수수료를 부가할 자격이 없다.
	리버스엔지니어 권리를 부여하지 않는다.		리버스엔지니어 권리를 부여하는 것이 필요하다. (per GPL).
	복제에 대한 권리를 부여하지 않는다.		복제에 대한 권리를 부여하는 것이 필요하다. (per GPL).
	장비 및 컨텐츠를 DRM으로 보호한다.		장비 및 컨텐츠를 DRM으로 금지하지 않는다.
	경우에 따라 특허출현 할 수 있다.		특허소송을 제기하지 않는다.
종합의견	ㅇ 프로젝트 라이선스인 Basic Proprietary Commercial License는 일반적인 상용 독점 라이선스로서 코드공개를 허용하지 않고 사용자들로 하여금 해당 코드에 대한 수정 및 복제, 리버스엔지니어링을 허용하지 않는 라이선스 임 ㅇ 분석결과 해당 프로젝트에는 48.95%의 OSS파일이 전체 혹은 부분 일치 형태로 결합 사용되었으며, 프로젝트 라이선스 의무사항과 직접 충돌 되는 라이선스인 GPL 2.0(24개파일, 4.8%), GPL3.0(116개파일, 23.2%)이 결합되어 있음 ㅇ 이는 GPL 계열에서 요구하고 있는 코드 배포(공개) 및 수정, 복제 권리를 사용자에게 허가해야 되는 의무사항이 발생됨 ㅇ 특히, GPL 3.0의 경우에는 장비 혹은 컨텐츠에 대한 접근권한을 사용자들에게 부여해야 함. 따라서, 해당 라이선스 코드에 대한 수정 및 삭제가 요구됨. ㅇ 또한, 프로젝트 라이선스와 직접 충돌은 되지 않고 있으나 Apache License 2.0코드가 포함되어 있음에 따라 해당 코드를 수정 및 삭제 하지 않고 결합 사용 시에는 사용자들에 대한 고지의무가 발생 됨, 기타 Opne SSL Combined License와 Sun Code Sample License는 코드를 공개하지 않는 한 별다른 의무사항은 발생되지 않음.		

© 2016. Black Duck Software Korea all rights reserved.

오픈소스 라이선스 검증 보고서

▣ 식별확인된 파일현황

License Conflict	File/Folder	Size	File Line	Total Lines	Component	Version	License	Usage	%	Matched File
다른 콤포넌트라이선스와 충돌	/lib/commons-collections.jar	165119			Apache Jakarta Commons Collections	2.1	Apache 1.1	Component	100%	bin/commons-collections-2.1.tar.gz/commons-collections-2.1/commons-collections.jar
프로젝트에 선언된 라이선스 와 충돌	/acmemail/acmemail.cgi	56824			Acmemail	Unspecified	GPL 2.0	File	100%	
프로젝트에 선언된 라이선스 와 충돌	/acmemail/AcmemailConfAbridged.pm	7328	4	147	Acmemail	Unspecified	GPL 2.0	Snippet	91%	

© 2016. Black Duck Software Korea all rights reserved.
BLACKDUCK

오픈소스 라이선스 주요 위반사례

Mark Radcliffe – Partner at DLA Piper

"오픈소스 소프트웨어를 자유롭게 사용할 수 있던 시대가 끝나가고 있다. 오픈소스 라이선스 조건을 준수하지 못하는 기업은 소송을 당할 수 있다는 의미다."

"오픈소스가 새로운 시대에 접어들고 있다. 서로 협력하고 공생하던 세계가 상업적인 세계로 바뀌고 있다. 일부 업체들이 오픈소스 소프트웨어에 특허 소프트웨어 같은 기준으로 권리를 행사하고 있다. 또 이를 전략적으로 사업에 활용하는 방안을 생각하고 있다"

"사람들이 '오픈소스 공동체에 제기될 수 있는 소송이 있을까'라고 생각했던 시대는 끝났다. "지금은 '오픈소스 프로젝트에 기여했으니, 이를 경쟁 무기로 사용해야지'라고 말하는 시대다"

© 2016. Black Duck Software Korea all rights reserved.

오픈소스 라이선스 주요 위반사례

- the future of Open Source 2016 리서치 결과에 의하면, 약 50%의 기업에서 오픈소스 도입 및 검토에 대한 공식적인 정책이 없음
- 오픈소스 도입 및 검토에 대한 정책을 가지고 있는 기업(약 50%)들 마저도, 오픈소스 도임 및 검토 정책을 제대로 수행하지 않거나 간과하는 경우가 많음

© 2016. Black Duck Software Korea all rights reserved.

오픈소스 라이선스 주요 위반사례

▣ 시사점을 주는 분쟁사례 소개

- ✓ 엘림넷 v. 하이온넷 : 최초의 국내 오픈소스 라이선스 관련 법정사례
- ✓ Jacobsen v. Katzer : 오픈소스 라이선스 위반이 저작권 위반이라는 미국 최초의 판결
- ✓ Welte v. Skype : 유통업체 책임 및 고지의무 준수에 독일 판결
- ✓ FSF v. Bracken : 합의문 조건을 인지할 수 있는 합의 사례
- ✓ Welte v. D-Link : 독일 및 대륙법 하에서 오픈소스 저작권을 인정한 판결
- ✓ FSF v. Cisco : 공급망 관리 필요성을 인지시켜준 합의 사례
- ✓ SFC v. 14개 기업 : 최초의 한국기업 관련 법정사례

© 2016. Black Duck Software Korea all rights reserved.

오픈소스 라이선스 주요 위반사례

▣ 최근 분쟁 사례 소개

- ✓ 삼성전자 exFAT
- ✓ Versata Software v. Ameriprise
- ✓ Patrick McHardy v. 다수의 유럽 제조 및 유통사
- ✓ Christoph Hellwig v. Vmware
- ✓ Google v. Oracle
- ✓ **Xiaomi**

▣ 기타 국내 분쟁사례 소개

- ✓ 다양한 라이선스, 비즈니스 관점에서의 국내 분쟁사례

© 2016. Black Duck Software Korea all rights reserved.

오픈소스 라이선스 주요 위반사례

엘림넷 v. 하이온넷

- 엘림넷의 핵심 솔루션인 ETUN의 개발자가 회사를 퇴사하고 HnP라는 회사를 창업하면서 ETUN을 개량한 HL 소프트웨어를 하이온넷에 제공
- 엘림넷이 하이온넷을 상대로 부정경쟁방지 및 영업비밀보호에 관한 법률위반으로 형사소송, 저작권침해가처분으로 민사소송을 제기함
- 소송의 핵심 대상인 ETUN이 GPL 라이선스인 Vtun을 모방한 것이 밝혀짐
- FSF는 서울중앙지방법원에 엘림넷과 하이온넷 모두 GPL을 위반했고 따라서, 영업비밀은 해당되지 않음을 제안
- 서울중앙지방법원은 FSF의 의견에도 불구하고 ETUN의 영업비밀에 해당되는 부분을 인정하였고 항소 진행 중(2005.9)
- 이후 FSF는 엘림넷과 하이온넷을 상대로 GPL 라이선스인 Vtun의 저작권위반과 관련하여 저작권자들을 대표하여 이의 제기
- 엘림넷과 하이온넷은 향후 GPL 준수를 약속하고 해당 소프트웨어에 대한 소스 전체를 공개
- 쟁점 및 시사점 :
  - 국내 최초의 GPL 라이선스 관련 소송 사건
  - 경쟁사간의 법정 소송
  - 법원 결과와 관련 없이 양사 모두 소송을 통해 원하는 결과를 얻지 못했으며, 사건의 핵심 솔루션에 대한 소스가 GPL 임을 인정하고, 엘림넷과 하이온넷은 공개 사과문을 발표하였고 GPL 규정에 따라 공개
  - 홈페이지를 통해 소스 전체를 공개 하였음

© 2016. Black Duck Software Korea all rights reserved.

오픈소스 라이선스 주요 위반사례

Jacobsen v. Katzer

- Jacobsen은 Java Model Railroad Interface(JMRI) 프로젝트를 리드하며, JRMI은 모형 기차 통제 소프트웨어인 DecoderPro를 개발, Artistic License 1.0 버전 하에서 배포
- 이 때, Artistic License 전문이 포함되어 있는 "COPYING" 파일을 참조하라는 저작권 공지를 포함시켰음
- Katzer는 Decoder Commander라는 유사 소프트웨어를 판매하는 Kamind Associates의 최고 경영자로, 상업용 소프트웨어 특허를 취득(2005.3)하였고, Jacobsen에게 DecoderPro의 배포를 중단할 것을 요구하였음
- JRMI는 이에 대응하는 중에 DecoderPro와 Decoder Commander의 코드가 비슷함을 발견
- 그러나 Decoder Commander의 파일들은 저작자 및 "COPYING" 파일 안에 저작권 공지를 언급하지 않았고, Jacobsen은 저작권 위반을 이유로 소송 제기
- Katzer는 나중에 DecoderPro를 복사였음을 인정
- 연방항소법원은 Artistic License 조항들이 강제성이 있는 저작권 조건이라고 판시하였고, 그러한 조건을 따르지 않고 저작물을 사용하거나 배포하거나 수정하거나 복사하는 것은 라이선스 범위를 벗어나는 것이라고 판시
- 쟁점 및 시사점 :
  - 오픈소스 라이선스의 조건을 위반하여 오픈소스를 사용한 경우, 위반자는 저작권 책임을 진다는 것을 인정한 미국에서의 최초 판결

© 2016. Black Duck Software Korea all rights reserved.

오픈소스 라이선스 주요 위반사례

Welte v. Skype

- 독일지방법원이 세계 최대 인터넷전화 업체인 스카이프가 오픈소스 라이선스인 GPL을 위반했다고 판결(2007.7.29)
- 스카이프 독일 지사가 유통한 인터넷 전화용 송수화기 'SMCWSKP100'에는 SMC라는 스페인 제조업체에서 펌웨어를 리눅스 기반으로 만들었음
- 법원은 "송수화기의 제조업체는 SMC지만, 스카이프가 이 제품을 실제적으로 웹사이트를 통해 판매했으므로 라이선스 요건 충족에 책임을 져야 한다"고 판결
- 법원이 GPL 위반을 결정 내린 배경은 GPL 기반 제품은 유통할 때, 사용자들이 소스 코드를 알 수 있도록 인터넷에 정보를 공개해야 하고, 해당 제품이 GPL 기반 제품이라는 것을 명시해야 함에도 불구하고 스카이프는 모두 지키지 않았음
- 스카이프는 이번 결정으로 SMCWSKP100의 소스 코드를 개방하고 벌금도 지불해야 함
- 금번 소송은 GPL 위반 여부를 감시하는 조직인 'gpl-violations.org' 산하 독일지부에서 제기됐고 이 조직은 2005년에도 보안업체 포리네트(Forinet)가 GPL을 어겼다고 소송을 제기, 소스 코드를 공개토록 유도한 바 있음
- 쟁점 및 시사점 :
  - 이번 사례는 제조업체뿐만 아니라, 유통업체에도 GPL 위반 책임을 물었다는 점
  - 본국이 아닌, 다른 나라에서도 얼마든지 GPL 위반에 대한 대가를 치르도록 했다는 점

© 2016. Black Duck Software Korea all rights reserved.

오픈소스 라이선스 주요 위반사례

FSF v. Bracken

- Bracken사의 제품은 주로 OEM 벤더들에게 판매되며, 응용장치에 설치되어 인터넷 브라우징 역할을 하는 장치같이 단일한 용도로 쓰임
- 제품은 거의 100% 자유소프트웨어이며, 대부분 GPL이나 관련된 라이선스 하에 배포된 것
- FSF는 Slashdot(뉴스제공 및 토론 사이트)에 기재된 리포트를 통해 위반내용을 인지하였고, 위반내용을 Bracken사에 제시하여 합의를 이끌어냈음
- 합의 및 협상 내용 :
  - Bracken사의 대리인은 EULA를 GPL에 맞게 재작성하여, 새로운 EULA의 이용 전 FSF를 통한 심사를 거칠 것
  - Bracken사의 엔지니어들은 GNU/Linux 배포판에 관한 소스를 제공할 것
  - Bracken 사의 대리인은 소스공개와 관련한 이러한 사태가 향후 재발하지 않도록 하기 위해, GPL의 준수를 위한 내부세미나를 엔지니어들 대상으로 운영할 것
  - Bracken사는 FSF가 공식적으로 당사의 배포권을 회복시킨 이후에만 상품 배포를 재개할 것

© 2016. Black Duck Software Korea all rights reserved.

오픈소스 라이선스 주요 위반사례

Welte v. D-Link

- 독일 프랑크푸르트 지방법원이 대만의 D-Link사에서 출시하고 있는 NAS 장비인 DSM-G600이 GPL 라이선스를 위반했다고 판결 (2006.6)
- 본 소송은 GPL-Violations에서 제기했고 본 판결을 통해 D-Link는 DSM-G600 판매를 중지하고 벌금은 물론 GPL-Violations에게 소송비용 일체와 테스트 장비 구입과 Reverse Engineering 비용을 부담해야 했음
- 쟁점 및 시사점 :
  - 독일법 아래에서 GPL의 법률적 구속력을 인정

© 2016. Black Duck Software Korea all rights reserved.

오픈소스 라이선스 주요 위반사례

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

HOW TO APPLY THESE TERMS TO YOUR NEW PROGRAMS

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.

This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

DGPLCODEDKD011

4 D-Link

D-Link

D-LINK GPL CODE STATEMENT

This D-Link product includes software code developed by third parties, including software code subject to the GNU General Public License ("GPL") or GNU Lesser General Public License ("LGPL"). As applicable, the terms of the GPL and LGPL, and information on obtaining access to the GPL code and LGPL code used in this product, are available to you at:

http://tsd.dlink.com.tw/GPL.asp

The GPL code and LGPL code used in this product are distributed WITHOUT ANY WARRANTY and is subject to the copyrights of one or more authors. For details, see the GPL code and the LGPL code for this product and the terms of the GPL and LGPL.

WRITTEN OFFER FOR GPL AND LGPL SOURCE CODE

Where such specific license terms entitle you to the source code of such software, D-Link will provide upon written request via email and/or traditional paper mail the applicable GPL and LGPL source code files via CD-ROM for a nominal cost to cover shipping and media charges as allowed under the GPL and LGPL.

Technical Support: For product support, please visit http://support.dlink.com for further assistance.

General Public License ("GPL") Inquiries: Please direct all GPL inquiries to the following email/ address. Note that technical support inquiries will not be supported at the below address.

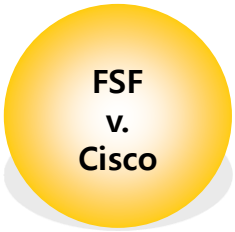
Email:
GPLCODE@DLink.com

Snail Mail:
Attn: GPLSOURCE REQUEST
D-Link Systems, Inc.
17595 Mt. Herrmann Street
Fountain Valley, CA 92708

D-Link 1

© 2016. Black Duck Software Korea all rights reserved.

오픈소스 라이선스 주요 위반사례



- 2008년 12월 11일, FSF는 Cisco를 상대로 GPL 2.0 및 LGPL 2.0 위반을 이유로 소송 제기
- 문제된 제품은 Broadcom이 Linksys에 제공한 것으로, Linksys를 Cisco가 인수하였기 때문에 현재 라이선스를 위반하고 있는 Cisco가 소송대상이 된 것
- 2009년 5월 20일 Cisco는 Linksys 제품이 자유소프트웨어 라이선스를 준수하는 것을 합의하였고, 또한 FSF에 비공개적 재정지원을 하는 것을 포함함으로써 양사가 합의
- 쟁점 및 시사점 :
  - 최초 위반자가 아니더라도 기업 인수등을 통해서 위반이 지속되는 경우 현재 위반을 하고 있는 회사가 책임을 져야한다는 점
  - 비슷한 예로, IBM은 Think Dynamics를 인수할때 GPL 위반사항을 발견하여 인수가액을 50%까지 낮추기도 했음

© 2016. Black Duck Software Korea all rights reserved.

오픈소스 라이선스 주요 위반사례

FSF v. Apple

- 2010년 5월 Free Software Foundation이 애플사에 GPL 위반에 대한 경고레터 발송
- 애플사의 사용자약관(EULA, End User License Agreement)가 GPL 조항을 위반함을 통지
- GPL Go 라는 앱이 애플 앱스토어에서 배포되고 있었는데 해당 앱은 GPL 2.0의 적용을 받음
- 앱 개발자에 대한 소스코드 공개 요구와 동시에 애플사에 GPL과 상충되는 사용자 약관 수정 요청
- 상충된 사용자 약관의 내용
  - GPL 2.0 제6조 추가적인 제한 금지 조항(NO FURTHER RESTRICTION)
  - 애플 사용자 약관의 경우 : 애플사가 정한 USAGE RULES에 따라서만 앱을 사용할 수 있고 5가지 기기에만 다운로드 받은 앱을 사용할 수 있도록 제한
- 애플의 대응 및 한계
  - 논란이 된 앱을 앱스토어에서 삭제
  - 해당 앱을 삭제함으로 인해 사용자약관과 GPL의 상충에 대한 법적 결론 도출 실패
  - 사용자 약관을 수정하지 않음으로 인해 GPL 적용이 된 앱의 경우 애플 앱스토어에서 유통이 사실상 어려움
  - 앱 개발자가 GPL을 위반한 경우 개발자도 의무사항을 준수해야 하지만 앱스토어의 운영자도 의무사항을 부담하게 되고 앱스토어에서 퇴출될 위험성 발생

- 쟁점 및 시사점
  - GPL 적용을 받는 앱의 자유로운 배포와 사용에 대해 추가적인 제한 금지
  - 이러한 의무는 앱개발자가 오픈소스 라이선스 상의 준수사항을 모두 이행한 경우에도 추가 적용가능

© 2016. Black Duck Software Korea all rights reserved.

오픈소스 라이선스 주요 위반사례

회사명	위반제품
BestBuy, Co., Inc	Insignia NS-WBRDVD Blu-ray Disc Player
Samsung Electronics America, Inc	LN52A650 , LA26A450 LCD HDTV
Westinghouse Digital Electronics, LLC	TX-52F480S LCD HDTV
JVC Americas Corporation	LT-42P789 LCD HDTV
	VN-C20U IP Network Camera
Western Digital Technologies, Inc	WDBABF0000NBK WD TV HD Media Player
Robert Bosch LLC	DVR4C Security System DVR
Phoebe Micro, Inc.	Airlink101 AR670W
	AR690W wireless routers
	Airlink101 AICAP650W IP Motion Wireless Camera
Humax USA Inc.	iCord HD HDTV DVR
Comtrend Corporation	CT-5621, NexusLink 5631/ 5631E ADSL2+ bonded modems
Dobbs-Stanford Corporation	Frame Jazz EyeZone B1080P-2 digital media player
Versa Technology Inc	PS-730 ITS Gateway
	VX-BW2250 weatherproof dual radio outdoor wireless access point
ZyXEL Communications Inc.	P-663H-51 ADSL 2+ Bonded 4 Port Router
Astak Inc	CM-818DVR4V security camera system with DVR,
	CM-04DE, CM-04DEV security system DVR devices
GCI Technologies Corporation	Cortex HDC-3000 digital music controller

© 2016. Black Duck Software Korea all rights reserved.

오픈소스 라이선스 주요 위반사례

삼성전자 exFAT

- **2013년 6월 25일,** 19살 유럽거주 A 여대생이 'GitHub'에 'exFAT' 파일시스템을 위한 리눅스 커널 드라이버를 업로드함
- 라이선스 문제를 명확히 하라는 요구에 A 여대생은 안드로이드 커널 3.0에서 얻은 것이며, 삼성소프트웨어 유출본 이라고 밝힘
- 삼성 저작권 침해라는 주장에 A 여대생은 해당 소프트웨어가 GPL 코드를 포함하고 있어 삼성전자가 GPL 라이선스에 따라 공개 했어야 한다고 반박
- 관련 업계 전문가들 사이에서 논쟁이 뜨거워짐
- 8월 16일, 삼성전자는 '삼성 오픈소스릴리즈센터'를 통해 'exFAT' 공개
- 소스코드 유출 경위 및 exFAT 드라이버 공개를 통해 야기될 수 이는 제 3자의 특허 침해 가능성(MS특허)등에 대해 논란 확산

© 2016. Black Duck Software Korea all rights reserved.

오픈소스 라이선스 주요 위반사례

Versata Software v. Ameriprise

- Versata는 특허 소프트웨어 제품인 DCM(Distribution Channel Management)에 XimpleWare라는 회사의 GPLv2로 라이선싱된 오픈소스 기반의 XML 파싱 유틸리티를 사용
- Versata는 Ameriprise라는 금융 서비스 회사에 DCM 소프트웨어를 라이선스하였음
- 그러나 Ameriprise가 하도급업체로 하여금 Versata와 경쟁하도록 소프트웨어를 디컴파일링 하도록 만들었고, 이것이 라이선스 위반이라고 주장하며 Ameriprise를 상대로 소송을 제기
- Ameriprise는 이에 맞서 Versata 소프트웨어는 GPLv2로 라이선싱된 오픈소스 소프트웨어가 포함되어 있고, 따라서 Versata 소프트웨어는 파생물로 간주되어 타 업체가 디컴파일링 및 수정할 수 있다는 주장을 근거로 소송을 제기
- GPLv2 라이선스 내용, 필수 저작권 통지 내용, 소스 코드 사본 등 GPLv2 소프트웨어에 통상 포함시켜야 할 내용 일체를 DCM의 오픈소스 부분에서 없앴다는 사실이 밝혀짐
- 이 사실을 알게된 XimpleWare는 Versata와 Ameriprise는 물론 Versata의 고객들을 저작권 및 특허권 침해로 고소
- 쟁점 및 시사점 :
  - 과거에는 오픈소스 소프트웨어 재단들이 오픈소스를 잘못 활용했다고 라이선스 침해를 주장하는 정도에 그쳤었으나 XimpleWare는 상업적 목적에서 이를 주장하였음
  - 이와 같이 오픈소스 소프트웨어 세계가 변화하기 시작했으며, 상업적 목적으로 이를 활용하는 사례가 증가할 가능성이 있고 이로인해 공급망 관리 필요성이 증대되고 있음

© 2016. Black Duck Software Korea all rights reserved.

오픈소스 라이선스 주요 위반사례

- 리눅스 커널 개발자인 Patrick McHardy는 2013년 12월부터 적극적으로 독일에서 GPL 소송 제기를 시작하였음
- McHardy는 리눅스 커널 네트워킹 스택, netfilter, iptables, iproute2, IMQ 그리고 nftables의 저작권을 보유하고 있음
- 대기업을 포함한 여러 기업체에 대한 저작권 침해 주장을 진행/합의 중
- 최근에는 채널/유통업체까지 타겟으로 삼고 있는 듯 함
- 기존의 라이선스 집행 사례와 상이한 점 :
  - 경제적인 동기로 진행중인 것으로 보여짐
  - 현재까지 합의된 건을 바탕으로 불안감 증대
  - 커널 기반의 저작권
  - 조잡한 "정지 명령" 편지와 컴플라이언스 엔지니어링
  - 짧은 기간 안에 반복되는 소송제기
  - 코드와 함께 라이선스를 배포하는 것에 대한 엄격한 견해
  - 적발된 기업이 아닌 McHardy와 그의 변호사가 먼저 합의조건을 제시
  - 컴플라이언스와 개선방안에 대한 의논이 없음

© 2016. Black Duck Software Korea all rights reserved.

오픈소스 라이선스 주요 위반사례

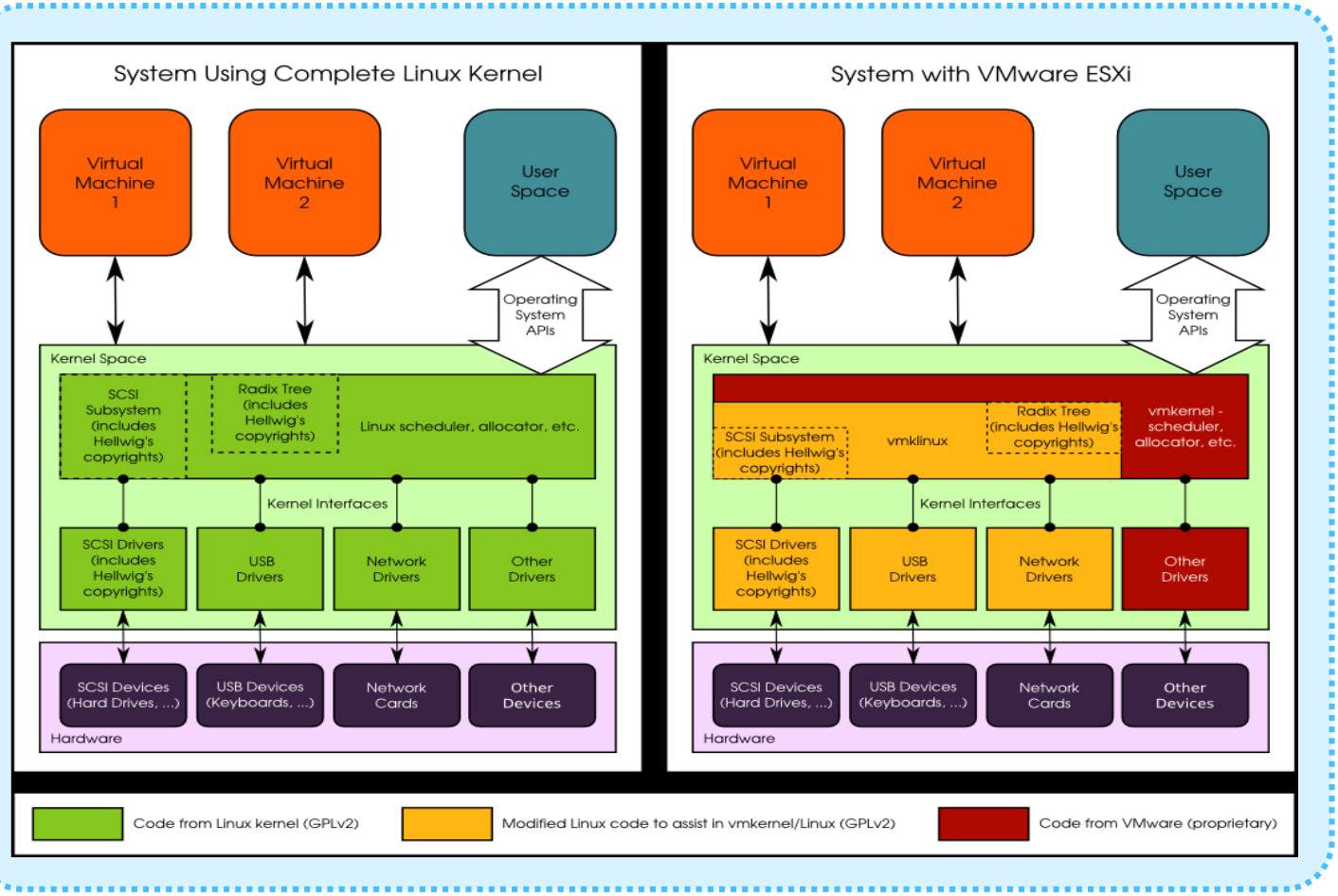
Hellwig v. VMware

- 2015년 3월 5일에 Software Freedom Conservancy (SFC)는 리눅스 커널 개발자인 Christopher Hellwig가 VMware를 상대로 함부르크 지방 법원에 소송을 제기하였음
- Hellwig는 VMware의 ESXi 제품이 리눅스 커널 내의 자신의 저작권을 침해한다고 주장
- 청구내용(Claims):
  - VMware ESXi의 커널 소스코드가 GPL v2.0에 의해 공개되지 않는다면 커널 배포에 대한 정지명령(Cease and desist)
  - 정지명령 관련으로 소비된 비용 청구
- 이 건의 경우 링크/결합물에 관한 문제 (뒷장 도표 참조) :
  - VMware의 ESXi는 리눅스 커널 모듈을 상용 커널에 로드함
  - VMware는 vmkernel과 리눅스 커널 코드 사이에 “shim”층을 사용하고 있을 수 있으며, VMware는 “shim”층이 있기 때문에 위반이 되지 않는다고 주장
  - Hellwig측은 결합방법의 기술적인 세부사항을 변경한다고하여 법적 해석이 바뀌는 것이 아니며, SFC의 조사에 따르면 VMware는 실제로 “shim”층을 사용하지 않는다고 주장함: “증거에 의하면 제품은 리눅스 코드와 vmkernel을 나란히 수정하여 결합하는 형식으로 개발된 것으로 보여진다.”
- 쟁점 및 시사점 :
  - 근본적으로, 정확히 어느 시점에서 두 프로그램이 결합이라고 정의내릴 수 있는지 법정에서 판결을 내려줘야할 것
  - “Linking”에 관한 문제는 오랫동안 논의되어 왔던 사항
  - 그러나 linking이 발생할 수 있는 여러 가지 상황이 있으며, 이 건은 그 중 일부의 경우에 대해서만 명확히 할 가능성이 있음

© 2016. Black Duck Software Korea all rights reserved.

오픈소스 라이선스 주요 위반사례

Hellwig v. VMware



© 2016. Black Duck Software Korea all rights reserved.

오픈소스 라이선스 주요 위반사례

Google
v.
Oracle

- 구글이 안드로이드 생태계를 형성하는 과정에서 자바 시스템을 부분적으로 도입하여 발생한 사건으로, 최초의 플랫폼 저작권 사건
- 구글이 저작권 보호를 받는 166개의 Java API 패키지들 중 37개를 취하여 그것들의 이름, 이름들의 구조(name organization), 기능성을 복제하여 제품에 그대로 사용한 후 저작권적 요소를 보완하기 위한 실행코드를 작성한 사건으로 축약될 수 있음
- 1심에서의 쟁점 :
  - API에 저작물성을 인정할 수 있는지
  - API에 '아이디어-표현 합체이론(merger doctrine)'을 적용할 수 있는지
- 2심에서의 쟁점 :
  - 오라클은 7천 줄의 선언 구문에 대해서는 문언적 침해를 주장
  - 37개의 Java API 패키지의 구조(structure), 시퀀스(sequence), 그리고 조직(organization)의 복제 에 대해서는 비문언적 침해를 주장
- 대법원 (2015. 6. 29) :
  - 상고 불허가
  - 1심 법원에서 다시 심리
  - 오라클은 2010. 12. 출시된 진저브래드부터 2014. 11. 나온 롤리팝까지 모든 안드로이드 버전이 자바의 저작권을 침해하였다며 자바 api 패키지가 없었다면 안드로이드가 제대로 구동되지 않을 것이라고 주장
- 쟁점 및 시사점 :
  - 구글의 오라클에 대한 책임이 인정될 경우 안드로이드 운영체제를 이용하여 휴대폰을 제조한 제조사, 안드로이드 운영체제를 이용한 애플리케이션 개발사에게도 책임이 인정될 것인지

© 2016. Black Duck Software Korea all rights reserved.

오픈소스 라이선스 주요 위반사례

- Xiaomi는 GPLv2 라이선스 위반으로 인해 많은 개발자들에게 비난받아 왔으며, 결국 문제가 되는 소스 코드를 라이선스 조항에 따라 공개하기로 결정
- 문제가 되는 부분은 Xiaomi기기에 사용되는 안드로이드 브랜치의 커널 소소 코드로, 안드로이드는 아파치 2.0 라이선스로 재배포시에 원본 소스 코드 또는 수정한 소스 코드를 반드시 공개되어야 하지는 않음
- 그러나 안드로이드의 기반이 되는 리눅스 커널은 아파치 라이선스에 해당하지 않으며 GPLv2 라이선스로 배포되고 있어 GPLv2의 속성에 따라 리눅스 커널 기반의 안드로이드 또한 GPLv2 라이선스를 갖게 됨
- 따라서 안드로이드를 사용하는 Xiaomi는 GPLv2 라이선스 조항 준수 의무가 발생하며 소프트웨어 수정 및 링크 시 모든 코드를 GPL에 의해 공개해야 함
- Xiaomi가 GPLv2 라이선스 조항을 준수하게 하기 위한 청원은 여러 번 이행되었으나, 오랫동안 준수되지 않고 있었음
- 2015년 3월 31일, Xiaomi는 Mi3, Mi4, 그리고 Mi Note의 소스 코드를 공개
- Mi3 (world, CDMA), Mi4, 그리고 Mi Note의 커널 소스 코드는 Xiaomi의 GitHub 페이지에서 확인할 수 있고, 아무나 열람 가능하며 이번 공개는 향후 커스템 ROM 에코시스템 발전에 기여할 것으로 기대됨

© 2016. Black Duck Software Korea all rights reserved.

오픈소스 라이선스 주요 위반사례

기타 국내 분쟁사례

- "타조 분쟁"
- ㈜그루터의 권영길 대표는, SK 텔레콤이 이 업체와 기술협력을 맺은 뒤, 핵심 기술인력과 몰래 거래하는 방식으로 피해를 입히고, 또한 이 기술을 SK 텔레콤이 "주도적으로 참여해 개발"한 것이라고 마케팅하여 업무를 방해받았다고 주장
- 그루터는 오픈소스 소프트웨어인 "아파치 타조"에 대한 기술지원을 제공하고 있는 업체로, "아파치 타조"에 관한 한 국제적인 명성을 얻을 정도로 중요한 공헌자로 평가받고 있음
- 그루터 권영길 대표의 주장 :
  - SK 텔레콤에서 타조 관련 솔루션을 다른 업체에도 적용시키는 대외사업을 시작하면서 그루터와 정식 라이선스로 기술지원 계약을 맺지 않고, 용역 방식을 요구하기에 거부
  - 후에 그루터의 CTO인 김모씨와 SK 텔레콤이 은밀한 거래를 했다는 의혹이 불거짐
  - 김 씨는 그루터의 핵심 기술인력으로 그를 직원이나 용역 인력처럼 사용할 수 있으면 SK 텔레콤은 그루터의 기술지원은 받지 않아도 될 정도
  - 실제로 김 씨는 그루터와 상관없이 SK 텔레콤의 기술 지원을 돕고 있는 것으로 밝혀졌고, 거래가 이뤄진 것인지는 확실하지 않음
- 이 사태에서의 문제점 :
  - 오픈소스에 대한 개념을 이해하지 못하고 있는 대기업 경영진
  - 오픈소스 제품에서조차 "원청-하청"이라는 갑을 관계로 끌고 가려는 관행
- 현재 권 대표는 미국내 기업들에게도 SK 텔레콤이 접촉해 업무를 방해한 행위들이 밝혀졌다고 주장하고 있고, 미국에서 징벌적 손해 배상 청구 소송이 가능한지 변호사를 통해 검토할 예정

© 2016. Black Duck Software Korea all rights reserved.

오픈소스 라이선스 주요 위반사례

기타 국내 분쟁사례

- "자동차"
- GPL V3.0

▣ 오픈소스 (OpenSource)검증 성적서 (오픈소스 등급 기준 표)

No.	라이선스 조항	적용여부
1	배포에 권리	●
2	배포/결합수준	●
3	소스코드의 배포/소스의 강제적 공유의 권리)	▲
4	사용자의 복제에 대한 권리	●
5	사용자의 수정에 대한 권리	●
6	사용자의 리버스 엔지니어에 대한 권리	▲
7	차별적 제한	●
8	수수료 (로열티 지급)	X
9	특허 보복	X
10	특정 특허 라이선스 (특허권 포기)	X
11	DRM 반대 조항	X
12	고지	●
13	필요한 변경사항 고지 (SW수정시 고지)	●
14	License Back (제작자 허락 필요)	X
15	보증 거부	●
16	책임의 한계	●
17	배상 의무사항	X
18	라이선스 전문 포함	●
19	프로모션 제약	▲
20	상호나눔/ 상호기여	▲
21	허가된 어플리케이션의 통합수준	GPL

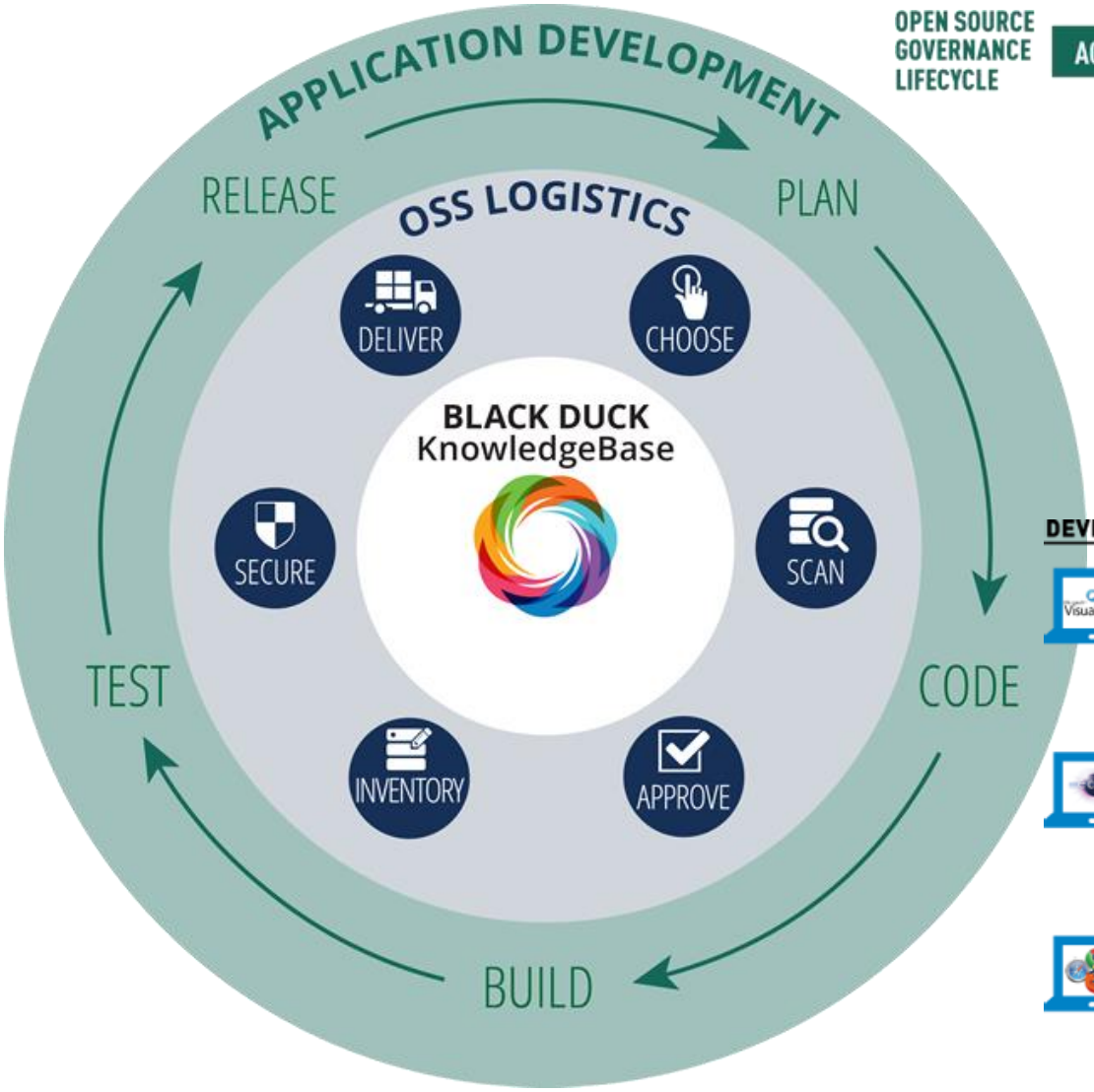
LEVEL	내용		HMC 권고사항
	설명	포함 항목	
1	Original	라이선스 사용 없음	권고 사항
2	Notice (●)	1,2,4,5,7 12,13,15,16,18	고지후 적용
3	Warning (▲)	3,6,19,20	항목 적용시 협의 필요 (실장전결)
4	Danger (X)	8,9,10,11 14,17	사용금지 사용 필요시 (센터장 전결)

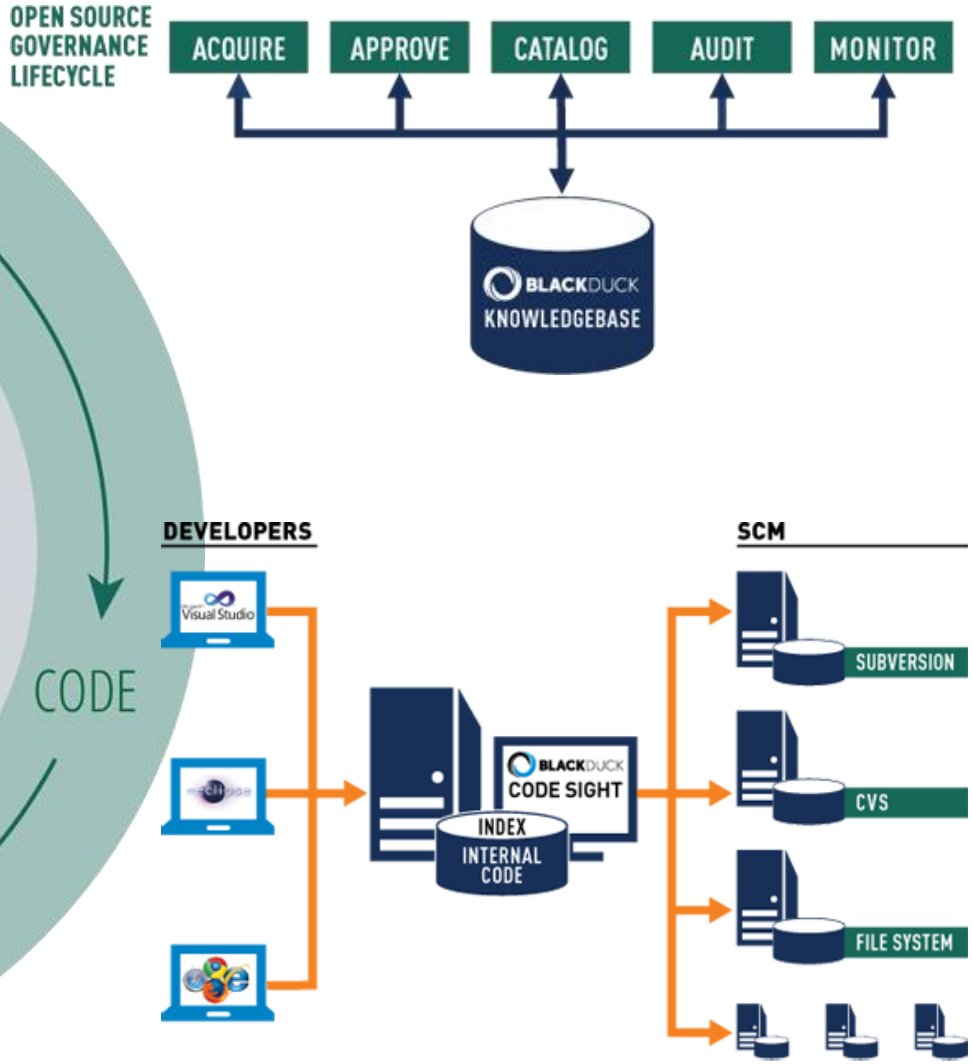
© 2016. Black Duck Software Korea all rights reserved.
BLACKDUCK

4. Black Duck Suite

© 2016. Black Duck Software Korea all rights reserved.

오픈소스 거버넌스 및 컴플라이언스 자동화 관리 솔루션
Black Duck Suite





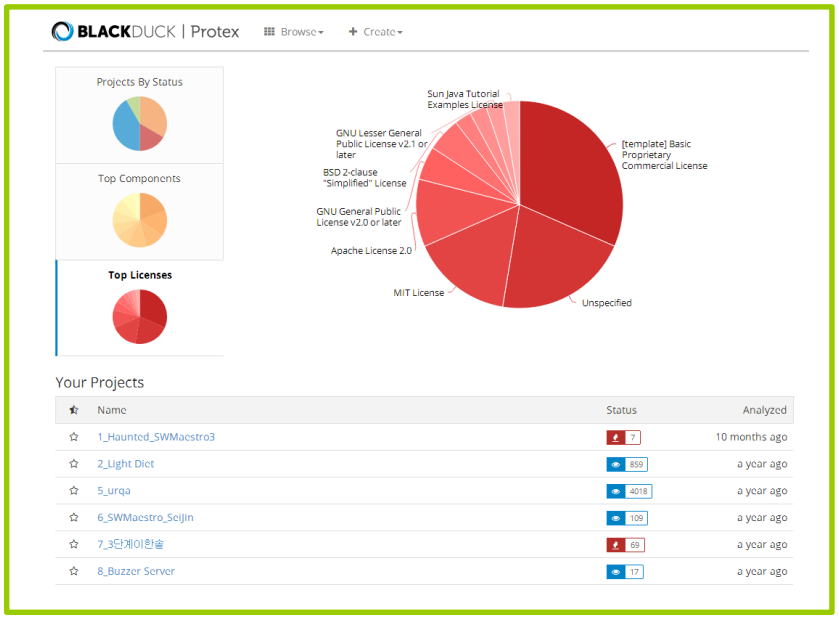
© 2016. Black Duck Software Korea all rights reserved.
BLACKDUCK

오픈소스 라이선스 검증 솔루션 Protex

Dashboard | My Protex | Manage | Identify | Review | Report

Protex를 통한 검증 데이트들을 종합하여 사용자가 쉽게 사용자의 오픈소스 사용 현황을 확인 할 수 있도록 대시보드를 제공

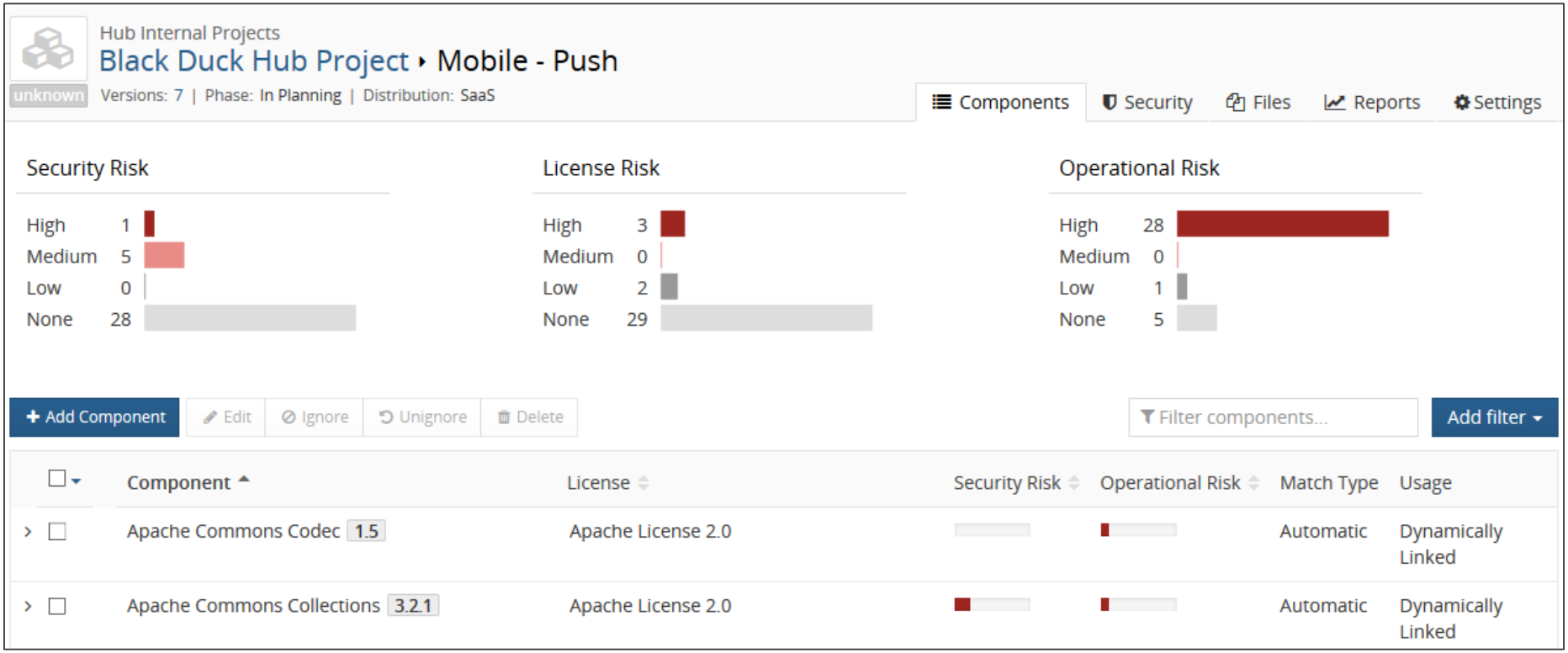
- **Top Components**
  - 팀 구성원 간 사용된 프로젝트에서 가장 많이 사용된 오픈소스 컴포넌트를 통계로 확인
- **Top License**
  - 팀 구성원 간 사용된 프로젝트에서 가장 많이 사용된 오픈소스 라이선스를 통계로 확인
- **Your Project**
  - 현재 사용 계정에 할당된 프로젝트 리스트 및 진행 현황을 확인할 수 있음



Protex 대시보드는 사용자의 데이터를 종합하여 현재 프로젝트 진행 상태와 함께 사용된 오픈소스 및 라이선스, 라이선스 위반 현황을 쉽게 파악하고 모니터링 할 수 있는 대시보드를 제공

© 2016. Black Duck Software Korea all rights reserved.
BLACKDUCK

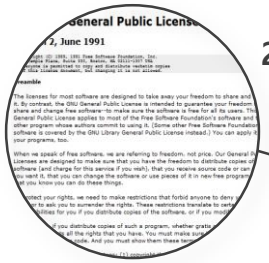
전사 오픈소스 포탈 Black Duck Hub



© 2016. Black Duck Software Korea all rights reserved.

BLACKDUCK

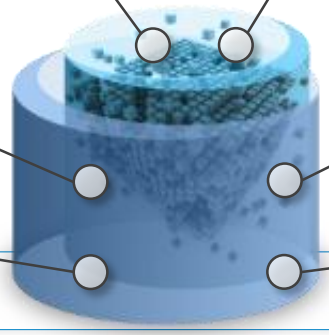
오픈소스 지식창구 Black Duck KnowledgeBase



2,400개 이상의
라이선스 정보

사용자 컴포넌트 구축
및 메타데이터

100만개 이상의 OSS 프로젝트
35억개 이상의 암호화된 코드
수백억 이상의 코드라인



60,000개 이상의
Security Vulnerability 정보

BLACK DUCK | KnowledgeBase
since 2002

8,500개 이상의 사이트에서
수집된 데이터

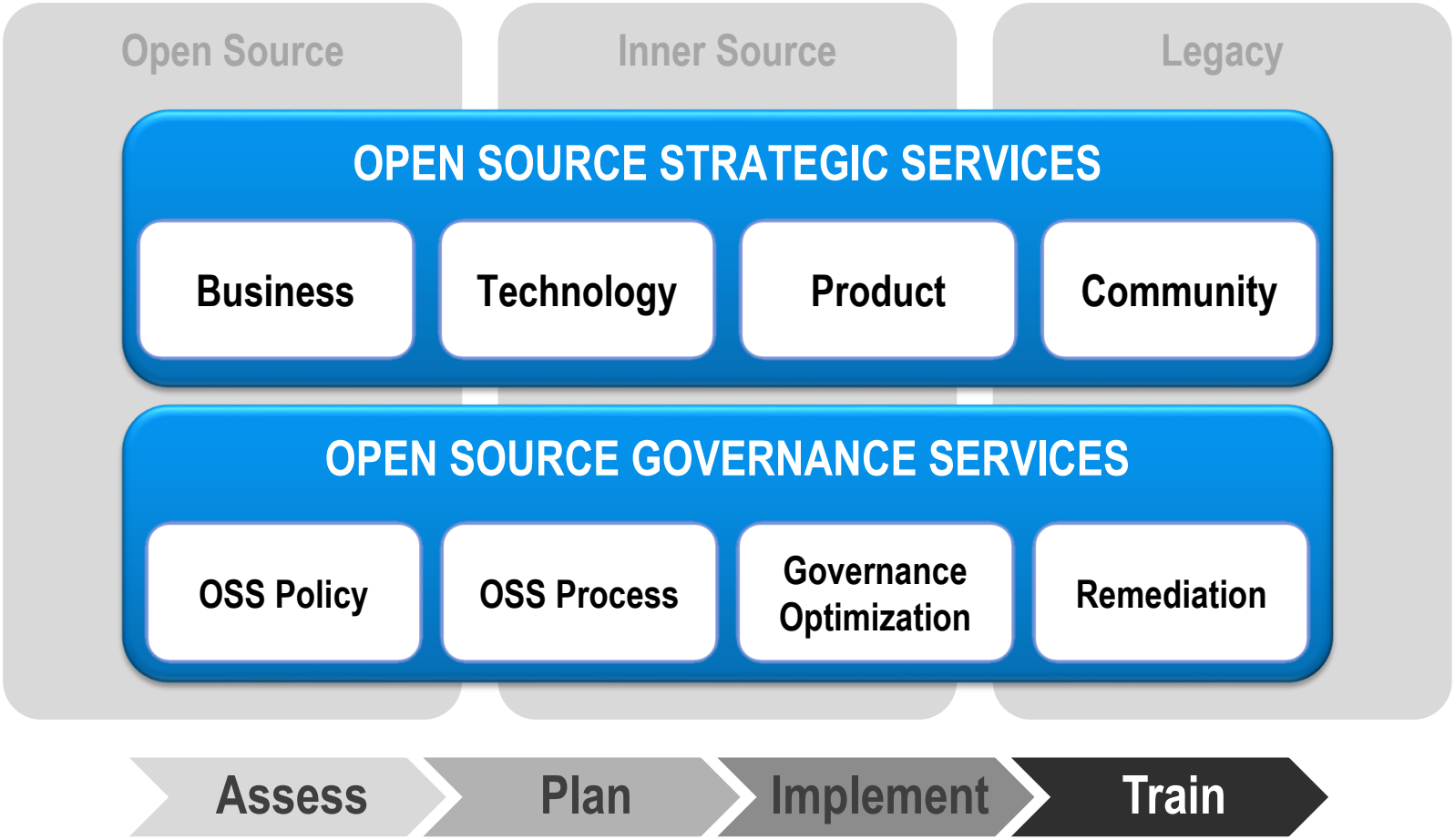
대규모 전담 KB 팀
및 프레임워크

지속적인 업데이트

Ohloh
300,000 OSS 개발자

© 2016. Black Duck Software Korea all rights reserved.
BLACKDUCK

블랙덕 서비스



Black Duck also offers custom open source industry research services

© 2016. Black Duck Software Korea all rights reserved.
BLACKDUCK

문의

BLACKDUCK

㈜블랙덕소프트웨어 코리아
김병선 상무
briankim@blackducksoftware.co.kr
(02)538-9227