기업에서의 컴플라이언스 리스크 관리와 실무 사례

kt ds 오픈소스SW팀

양한주

2015. 12. 03

kt ds

기업 환경의 변화

전통적인 통신 서비스에서 IT 융합 서비스로 영역 확장

전통적 통신 서비스

IT 융합 서비스

기업 환경의 변화

다양한 서비스의 증가는 수 많은 IT시스템 인프라를 요구함

전화국 교환원의 모습(서울신문)

현재의 데이터 센터
(http://www.madeinalabama.com/assets/2015/06/Google-Data-Center-Okla.jpg)

IT서비스의 증가와 비용에 대한 고민

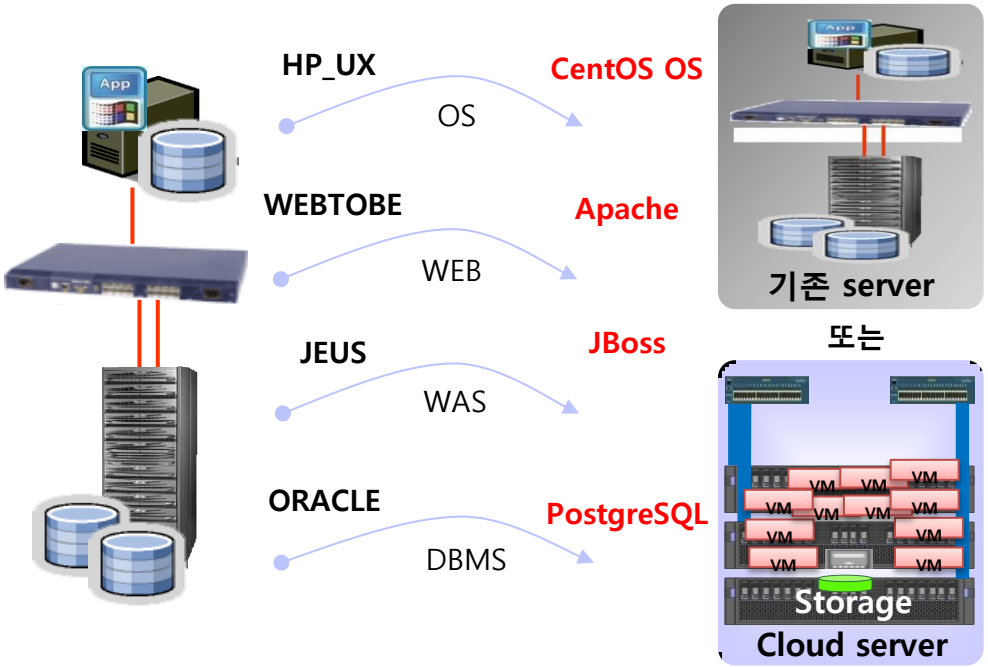
증가하는 IT시스템에 비례하여 SW에 대한 비용도 지속적으로 증가

- 시스템 증설에 따른 **추가 라이선스 구매**
- End of Service Life에 의한 **Upgrade 필요**
- 라이선스 비용 외 **높은 유지보수 비용**
- 솔루션 폐쇄성으로 인한 **벤더 종속성**
- Under License의 **Penalty 부담 및 소송비용**

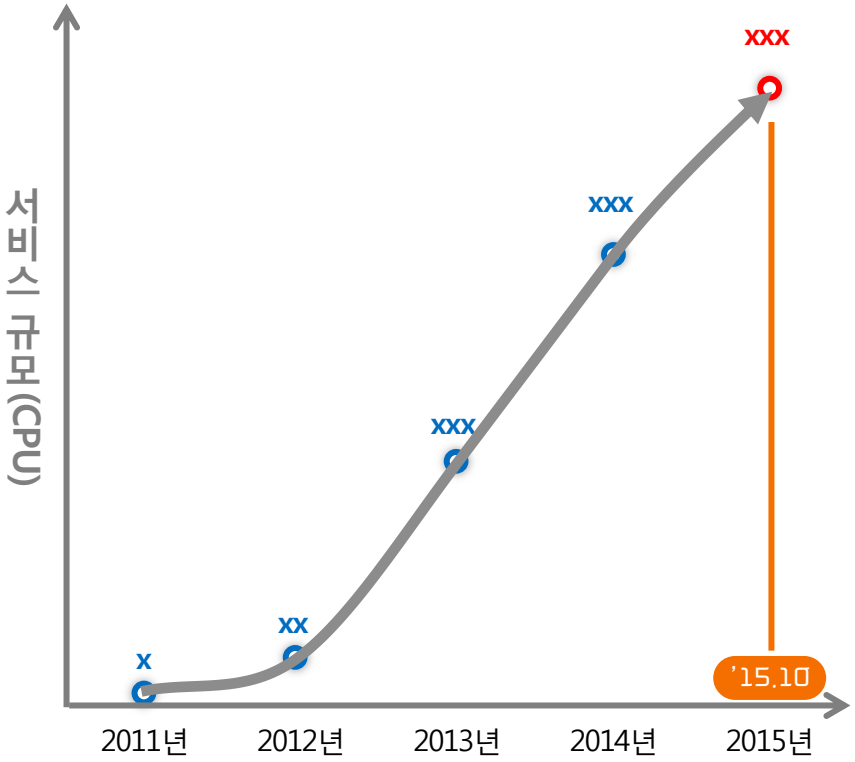
인프라 SW의 오픈소스SW 도입

기업 인프라의 상용 SW를 오픈소스SW 기반으로 전환

상용SW의 전환

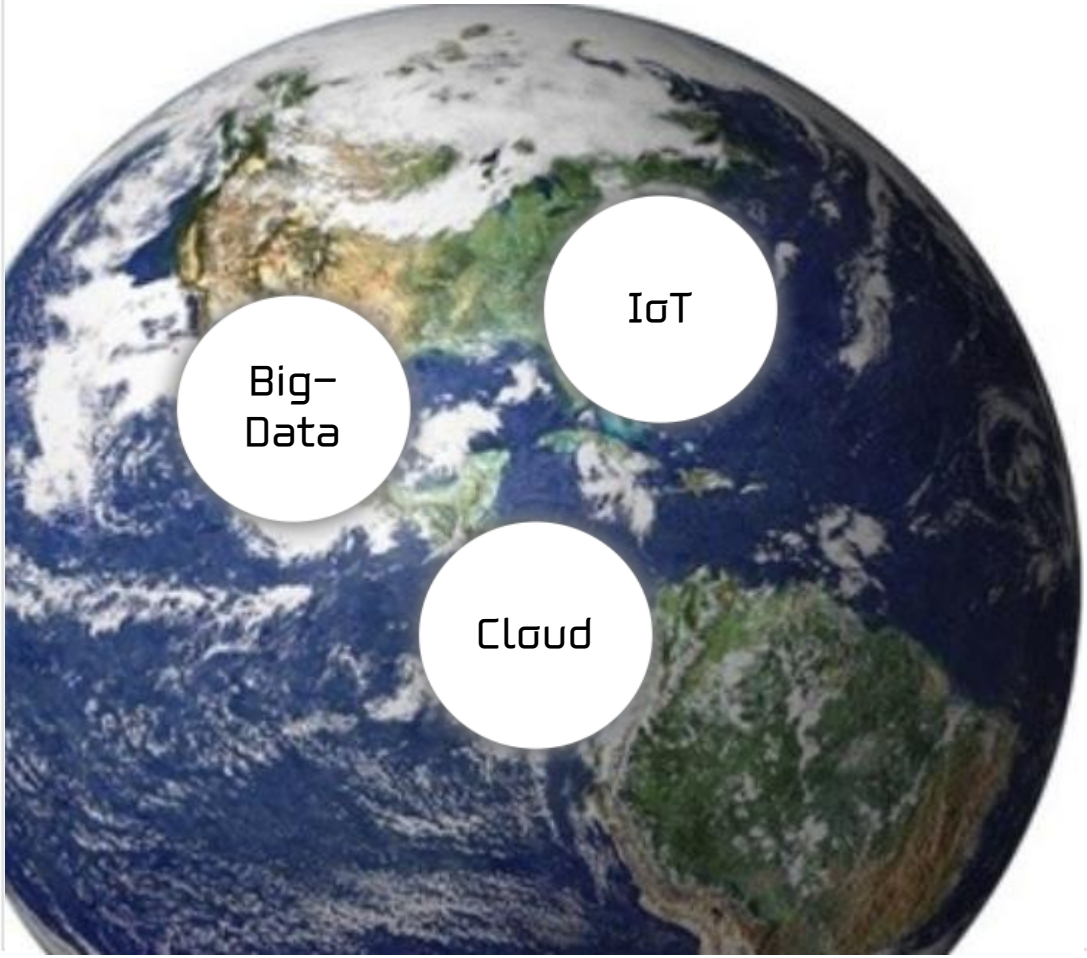


kt 그룹 오픈소스DB 도입 현황



어플리케이션 영역으로의 확장

기술의 발전과 트렌드에 민감한 IT영역의 오픈소스SW에 대한 폭넓은 수용과 지원 요구, 이로 인한 컴플라이언스 대응 필요성 부각



컴플라이언스??

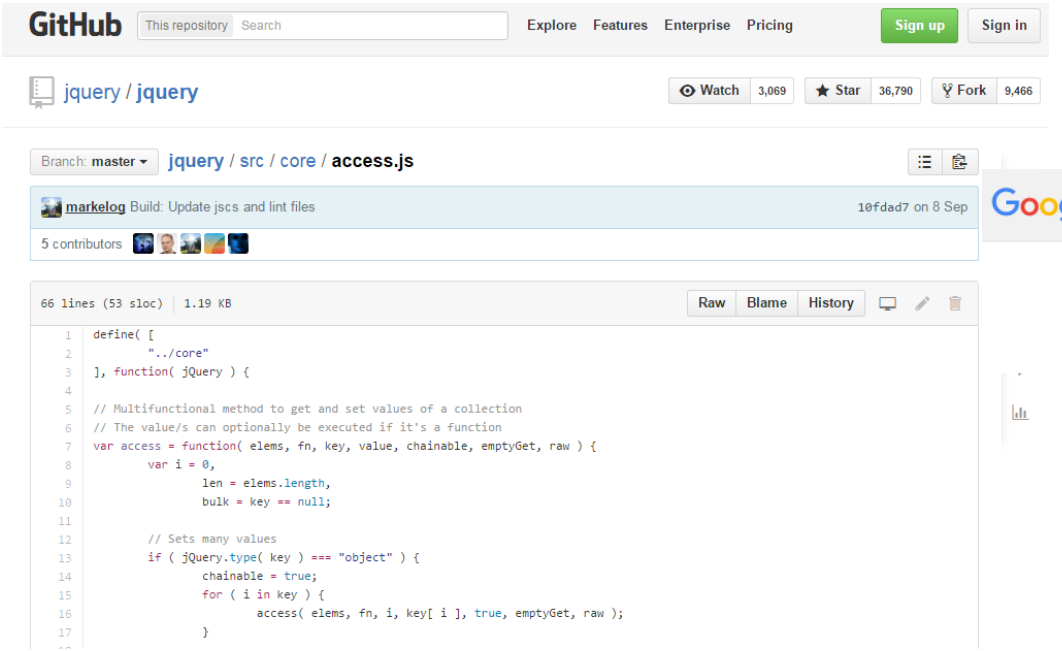
오픈소스SW의 정의

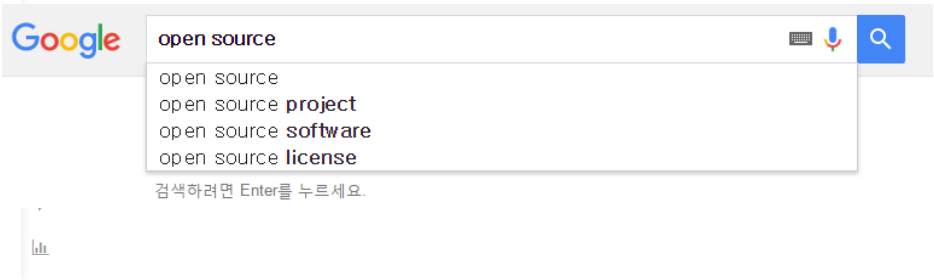
오픈소스SW의 정의는 시각에 따라 다양하게 해석될 수 있음

오픈소스SW는 소스코드가 공개되어 누구나 복제, 설치, 사용, 변경, 재 배포가 가능한 프로그램.

일반적으로 OSI(Open Source Initiative)의 10가지 조건을 충족해야 함

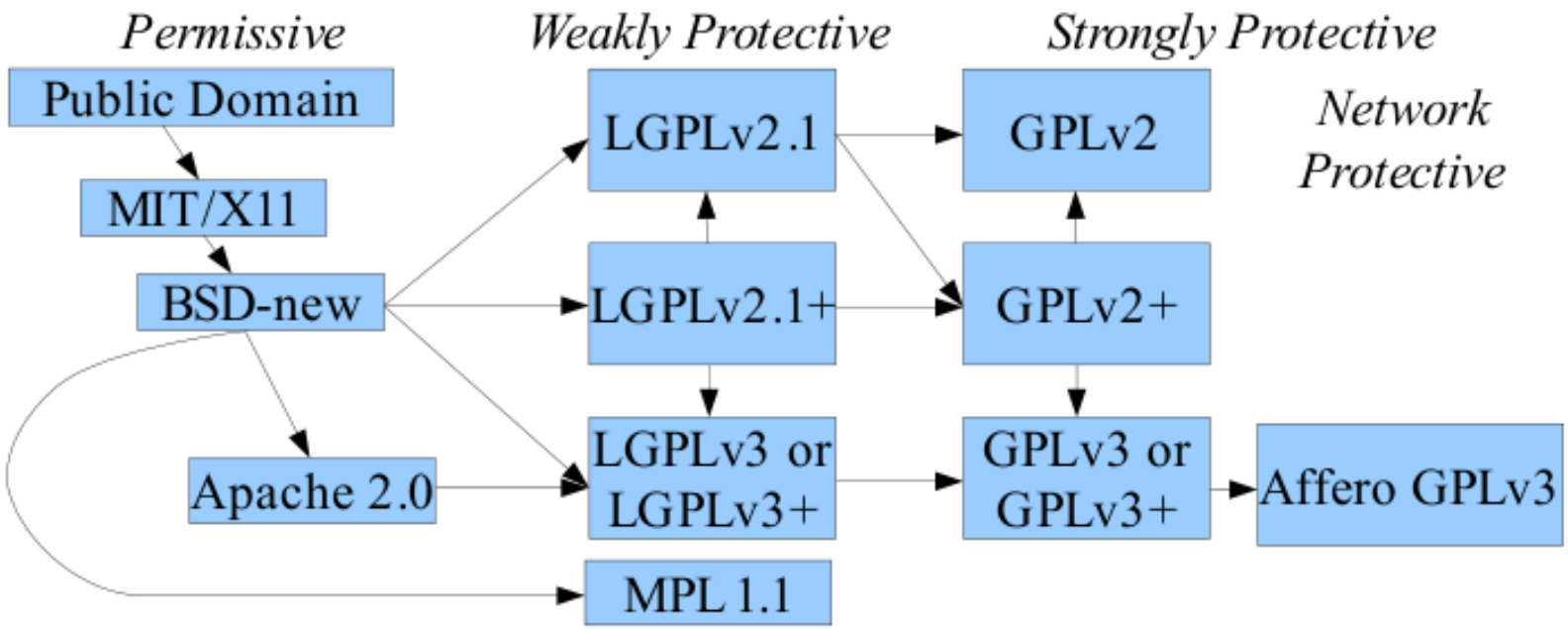
실제 개발자에게는?





오픈소스SW 라이선스

오픈소스SW 또한 저작권이 있으며, 복잡한 라이선스 정책은 많은 이슈를 발생 시킴



ref. www.dwheeler.com/essays/floss-license-slide.pdf

라이선스 위반 유형

대부분의 라이선스 위반 행위는 개발자의 실수나 무지에서 비롯됨

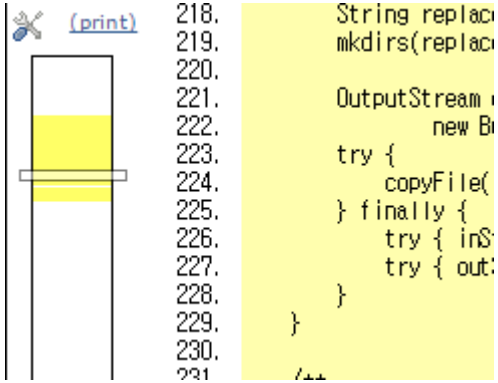
I 라이선스 삭제


```
/*! Copyright (c) 2011 Piotr Rochala (http://rocha.la)
 * Dual licensed under the MIT (http://www.opensource.org/licenses/mit-license.php)
 * and GPL (http://www.opensource.org/licenses/gpl-license.php) licenses.
 *
 * Version: 1.3.0
 *
 */
```

II 저작권 정보 변경/삭제

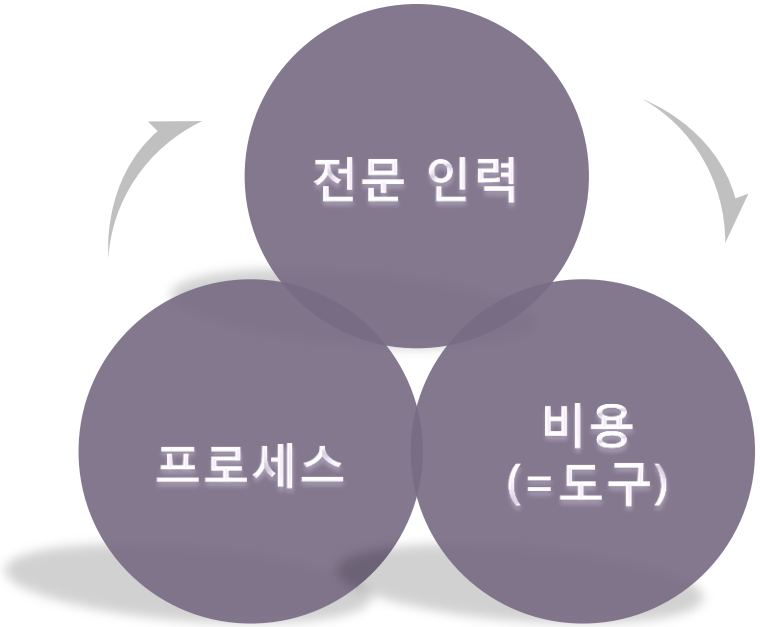
```
/*****************************************************************************
 * *   vWindow version 1.0
 * *
 * * Copyright © 2015    corp. All rights reserved.
 * *
 * * This is a proprietary software of    corp, and you may not use this file except in
 * * compliance with license agreement with    corp. Any redistribution or use of this
 * * software, with or without modification shall be strictly prohibited without prior written
 * * approval of    corp, and the copyright notice above does not evidence any actual or
 * * intended publication of such software.
 *****************************************************************************/
```

III 코드조각 임의 복제



오픈소스SW 컴플라이언스

What do we need ?



blackduck

PALAMIDA™
Application Security for Open Source Software

protecode

OpenLogic
a Rogue Wave Company

fossology

오픈소스SW 컴플라이언스

Why did we start?

The GNU General Public License (GPL)

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Apache Li
Version 2.0, Ja 004

http://www.a es/

TERMS AN USE, REPRODUCTION, AND DIS ON

1. De

ditions for use, reproduction, a ned by Sections 1 through 9 of this document.

ntity authorized b t is granting the License.

ol, are controlled by, or are under common control with that
direct, to cause the direction or management of such entity, whether
utstanding shares, or (iii) beneficial ownership of such entity.

an in ions granted by this License.

an the preferred form tions, including but not limited to software source code, documentation source

shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compil
erated documentation, and conversions to other media types.

ork" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright not
included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the edito
revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this Licens
Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Deriv
Works thereof.

Eclipse Public License - v 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS ECLIPSE PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and
b) in the case of each subsequent Contributor:

i) changes to the Program, and

ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents " mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

The MIT License

Copyright (c) <year> <copyright holders>

Permission is hereby granted, free of charge, to any person obtaining a c
"Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

단계별 검증 체계 구축

전사 라이선스 검증 및 관리를 위한 단계적 계획 추진

I 검증 체계 구축

1단계[도입]

- 검증 도구를 활용하여 오픈소스SW 라이선스 검증 프로세스 도입
- 오픈소스SW사용 현황 분석

II 관리 체계 구축

2단계[확산]

- 전사 및 협력사에 대한 관리정책 수립
- 표준화된 프로세스 설계를 통해 전사 관리 체계 구축

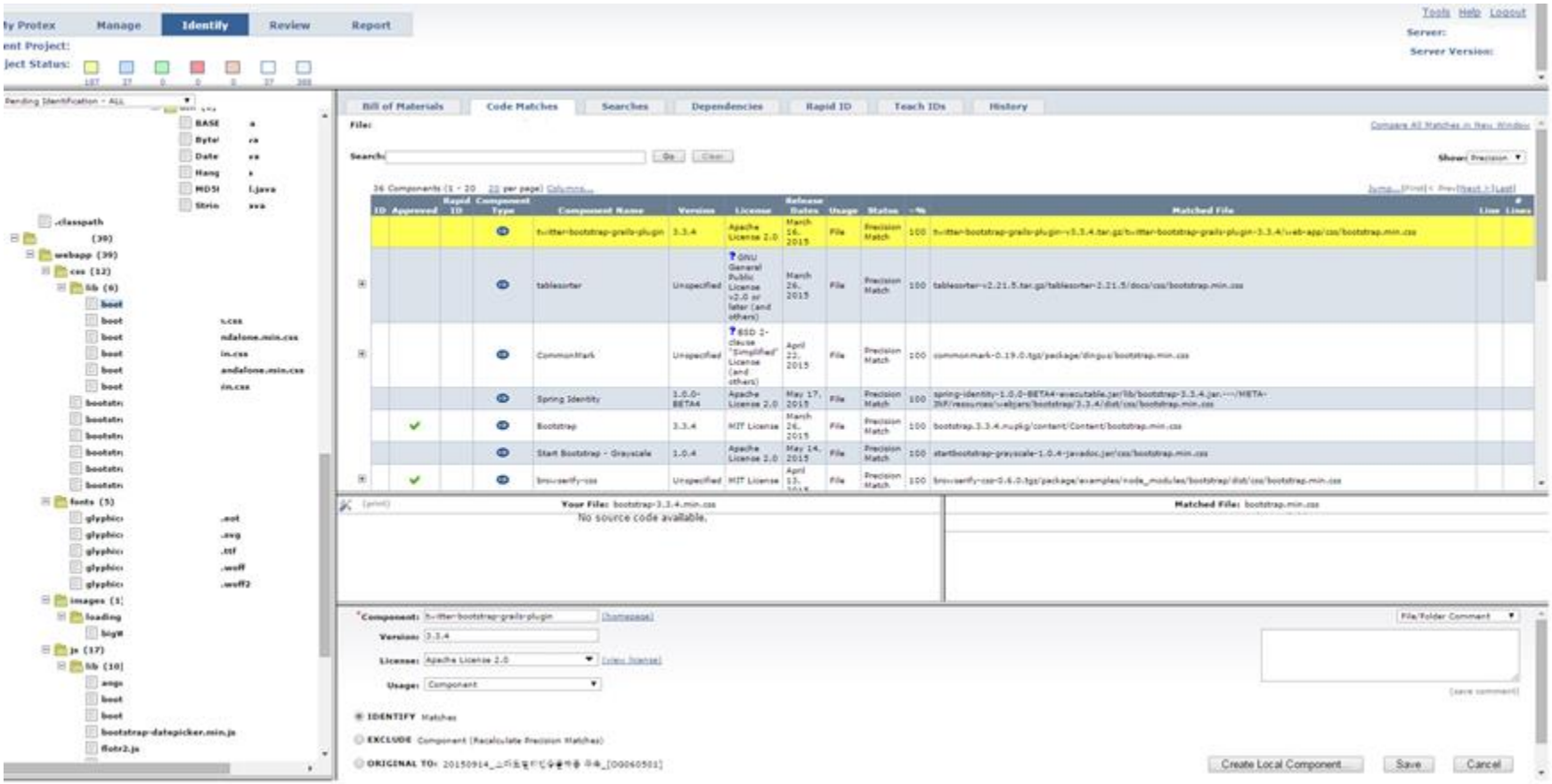
III 자산화 체계 구축

3단계[정착]

- 검증 및 승인된 오픈소스SW의 전사 통합 저장소 운영
- 그룹사 오픈소스SW 통합 관리 체계 운영

검증 도구의 활용

검증 도구가 모든 것을 해결해 주지는 않는다!



오픈소스SW의 범위와 판단

어떠한 기준으로 판단할 것인가?

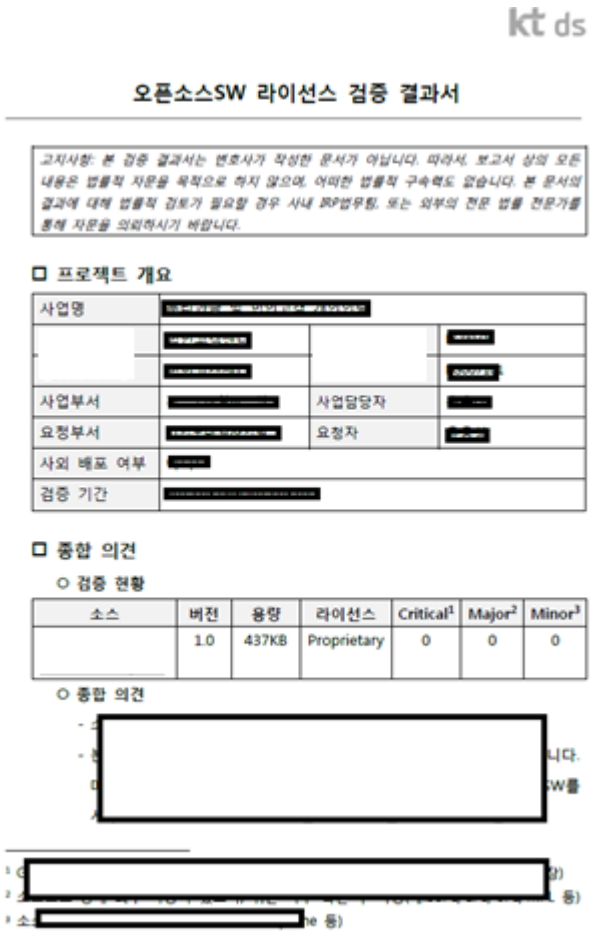
(print)

```java
/**
 * Usage:
 * String crypto = Crypto.encrypt(masterpassword, cleartext)
 * String cleartext = Crypto.decrypt(masterpassword, crypto)
 *
 */
public class Crypto {

    private final static String HEX = "0123456789ABCDEF";

    public static String encrypt(String seed, String cleartext) throws Exception {
        byte[] rawKey = getRawKey(seed.getBytes());
        byte[] result = encrypt(rawKey, cleartext.getBytes());
        return toHex(result);
    }

    public static String decrypt(String seed, String encrypted) throws Exception {
        byte[] rawKey = getRawKey(seed.getBytes());
        byte[] enc = toByte(encrypted);
        byte[] result = decrypt(rawKey, enc);
        return new String(result);
    }

    /*private static byte[] getRawKey(byte[] seed) throws Exception {
        KeyGenerator kgen = KeyGenerator.getInstance("AES");
        SecureRandom sr = SecureRandom.getInstance("SHA1PRNG");
        sr.setSeed(seed);
        kgen.init(128, sr); // 192 and 256 bits may not be available
        SecretKey skey = kgen.generateKey();
        byte[] raw = skey.getEncoded();
        return raw;
    }*/

    private static byte[] getRawKey(byte[] seed) throws Exception {
        KeyGenerator kgen = KeyGenerator.getInstance("AES"); // , "SC");
        SecureRandom sr = null;
        if (android.os.Build.VERSION.SDK_INT >=  17) {    //JELLY_BEAN_MR1 = 17
            sr = SecureRandom.getInstance("SHA1PRNG", "Crypto");
        } else {
            sr = SecureRandom.getInstance("SHA1PRNG");
        }
        sr.setSeed(seed);
        try {
            kgen.init(128, sr);
            // kgen.init(128, sr);
        } catch (Exception e) {
            // Log.w(LOG, "This device doesn't suppor 256bits, trying 192bits.");
            try {
```

```java
 * String crypto = SimpleCrypto.encrypt(masterpassword, cleartext)
 * ...
 * String cleartext = SimpleCrypto.decrypt(masterpassword, crypto)
 * </pre>
 * @author ferenc.hechler
 */
public class SimpleCrypto
{
    private final static String HEX = "0123456789ABCDEF";

    public static String encrypt(String seed, String cleartext) throws Exception
    {
        byte[] rawKey = getRawKey(seed.getBytes());
        byte[] result = encrypt(rawKey, cleartext.getBytes());
        return toHex(result);
    }

    public static String decrypt(String seed, String encrypted) throws Exception
    {
        if(!TextUtils.isEmpty(encrypted))
        {
            byte[] rawKey = getRawKey(seed.getBytes());
            byte[] enc = toByte(encrypted);
            byte[] result = decrypt(rawKey, enc);

            return new String(result);
        }
        else
            return "";
    }

    private static byte[] getRawKey(byte[] seed) throws Exception
    {
        KeyGenerator kgen = KeyGenerator.getInstance("AES");
        SecureRandom sr = SecureRandom.getInstance("SHA1PRNG");
        sr.setSeed(seed);
        kgen.init(128, sr); // 192 and 256 bits may not be available
        SecretKey skey = kgen.generateKey();
        byte[] raw = skey.getEncoded();
        return raw;
    }

    private static byte[] encrypt(byte[] raw, byte[] clear) throws Exception
    {
        SecretKeySpec skeySpec = new SecretKeySpec(raw, "AES");
        Cipher cipher = Cipher.getInstance("AES");
        cipher.init(Cipher.ENCRYPT_MODE, skeySpec);
        byte[] encrypted = cipher.doFinal(clear);
```

검증 결과에 대한 조치

요청자가 명확한 조치 사항을 확인할 수 있도록 요약된 라이선스 검증 결과서 제공



kt ds

오픈소스SW 라이선스 검증 결과서

고지사항: 본 검증 결과서는 변호사가 작성한 문서가 아닙니다. 따라서, 보고서 상의 모든 내용은 법률적 자문을 목적으로 하지 않으며, 어떠한 법률적 구속력도 없습니다. 본 문서의 결과에 대해 법률적 검토가 필요할 경우 사내 IRP(법무팀), 또는 외부의 전문 법률 전문가를 통해 자문을 의뢰하시기 바랍니다.

□ 프로젝트 개요

사업명	[redacted]		
	[redacted]		[redacted]
	[redacted]		[redacted]
사업부서	[redacted]	사업담당자	[redacted]
요청부서	[redacted]	요청자	[redacted]
사외 배포 여부	[redacted]		
검증 기간	[redacted]		

□ 종합 의견

○ 검증 현황

소스	버전	용량	라이선스	Critical[1]	Major[2]	Minor[3]
	1.0	437KB	Proprietary	0	0	0

○ 종합 의견

- [redacted]

- 라이선스의 구분
  - Critical, Major, Minor 3등급
- 구체적인 조치 사항 기술
  - 소스코드 공개 의무, 라이선스 고지 사항
- 기타 이슈 사항
  - 소스코드의 보안 취약 사항 등

라이선스 고지

복잡한 라이선스 고지문 생성

daumkakao 라이선스 고지문 생성기

daumkakao / legal-notice

Watch 4

Notification template for used list of open source libraries and components

5 commits | 2 branches | 0 releases | 1 contributor

Branch: master | legal-notice / +

Edit 3rd party libraries table

hooney authored on 5 Jun — latest commit 3d7e8aa2fa

ServiceName-PlatformName	first commit	3 months ago
lib	first commit	3 months ago
license	first commit	3 months ago
CONTRIBUTING.md	first commit	3 months ago
LICENSE.txt	first commit	3 months ago
README.md	Edit 3rd party libraries table	3 months ago

README.md

Legal Notice Template

This is notification template for used list of open source libraries and components.

github.com/daumkakao/legal-notice

OSS Notice | ServiceName for PlatformName Create .html

This application is Copyright © 2015, daumkakao corp. All Rights Reserved.

This application use Open Source Software (OSS). You can find the source code of these open source projects, along wit

Any questions about our use of licensed work can be sent to oss@daumkakao.com

ActionBarSherlock
http://github.com/JakeWharton/ActionBarSherlock/
Copyright © 2012 Jake Wharton
Apache License 2.0

Android Open Source Project (AOSP)
- *developers - samples - android*
- *packages - apps - Camera*
- *frameworks - volley*
- *SDK Support Libraries*
- *Support Library (v4)*

https://android.googlesource.com
Copyright © 2007-2015 The Android Open Source Project
Apache License 2.0

Apache HttpComponents
http://hc.apache.org/
Copyright © 2005-2015 The Apache Software Foundation
Apache License 2.0

JSON-java
http://github.com/douglascrockford/JSON-java/
Copyright © 2015 Douglas Crockford
MIT License

Apache License 2.0

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

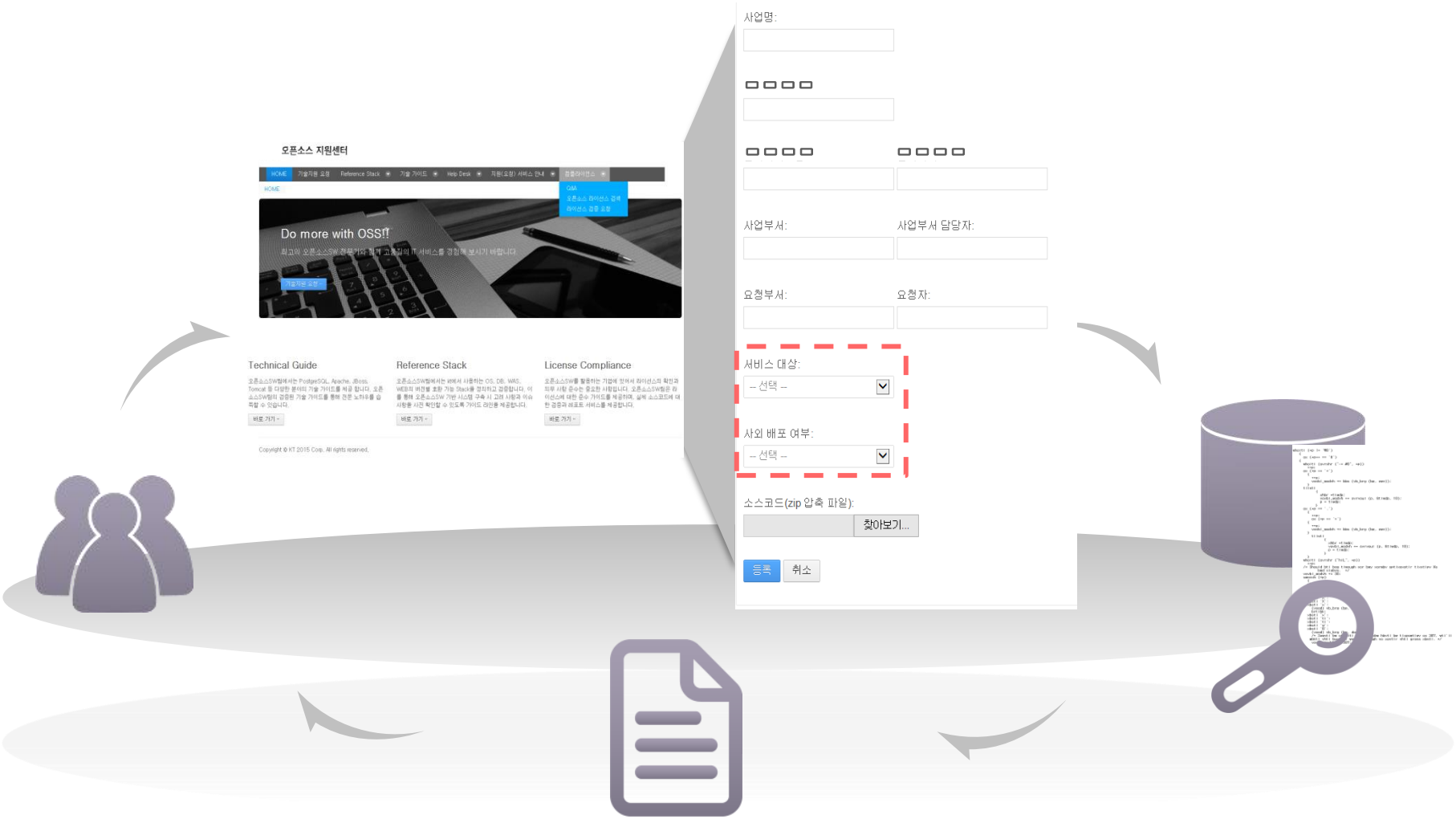
"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under p of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

커뮤니케이션

효율적인 커뮤니케이션과 관리의 필요성



내부적인 고민과 판단

책 사주세요. 라이선스

Copyright (C) 2001-2009 by Jason Hunter, jhunter_AT_servlets.com.
All rights reserved.

The source code, object code, and documentation in the com.oreilly.servlet package is copyright and owned by Jason Hunter.

ON-SITE USE RIGHTS

Permission is granted to use the com.oreilly.servlet.* packages in the development of any non-commercial project. For this use you are granted a non-exclusive, non-transferable limited license at no cost.

For a commercial project, permission is granted to use the com.oreilly.servlet.* packages provided that every person on the development team for that project owns a copy of the book *Java Servlet Programming* (O'Reilly) in its *most recent edition*. The most recent edition is currently the 2nd Edition, available in association with Amazon.com at http://www.amazon.com/exec/obidos/ASIN/0596000405/jasonhunter.

Other (sometimes cheaper) license terms are available upon request; please write to jhunter_AT_servlets.com for more information.

REDISTRIBUTION RIGHTS

Commercial redistribution rights of the com.oreilly.servlet.* packages are available by writing jhunter_AT_servlets.com.

Non-commercial redistribution is permitted provided that:

1. You redistribute the package in object code form only (as Java .class files or a .jar file containing the .class files) and only as part of a product that uses the classes as part of its primary functionality.

2. The product containing the package is non-commercial in nature.

3. The public interface to the classes in the package, and the public interface to any classes with similar functionality, is hidden from end users when engaged in normal use of the product.

4. The distribution is not part of a software development kit, operating system, other library, or a development tool without written permission from the copyright holder.

5. The distribution includes copyright notice as follows: "The source code, object code, and documentation in the com.oreilly.servlet package is copyright and owned by Jason Hunter." in the documentation and/or other materials provided with the distribution.

6. You reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.

7. Licensor retains title to and ownership of the Software and all enhancements, modifications, and updates to the Software.

Note that the com.oreilly.servlet package is provided "as is" and the author will not be liable for any damages suffered as a result of your use. Furthermore, you understand the package comes without any technical support.

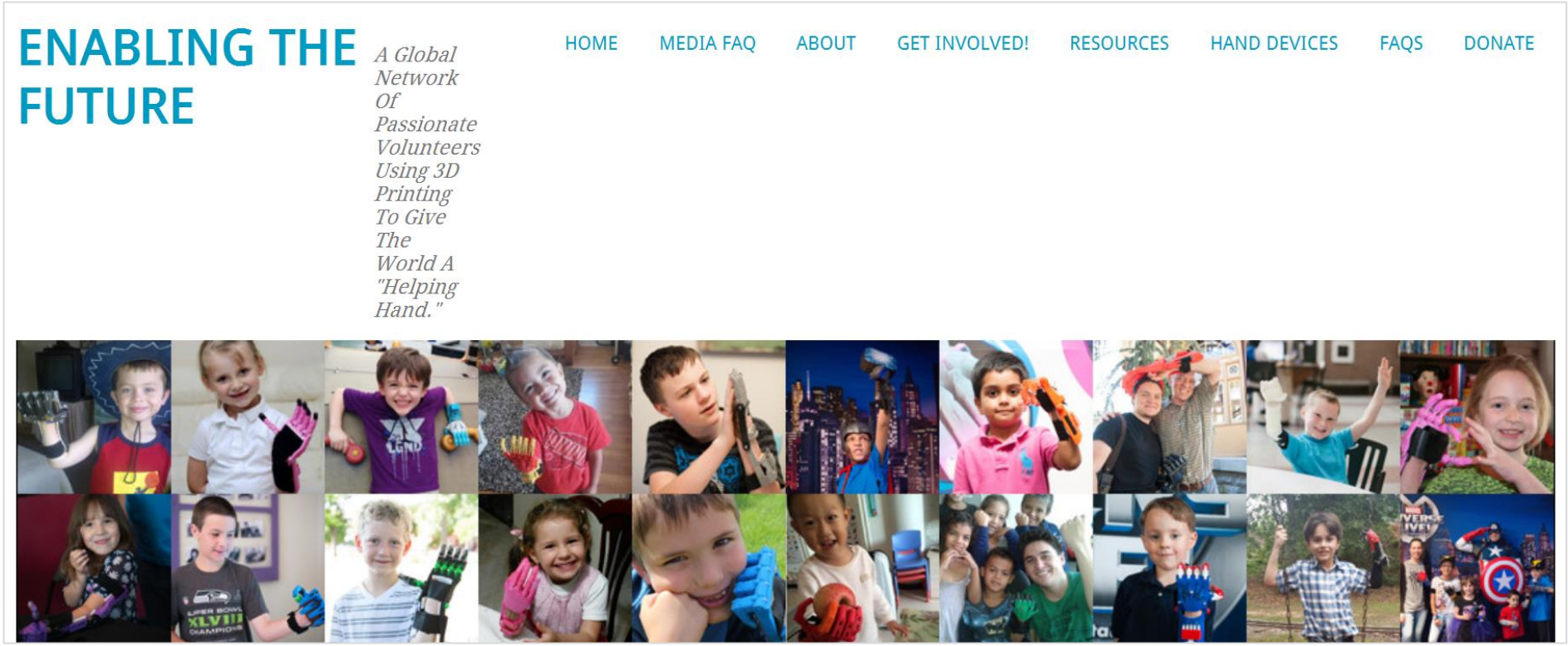
내부적인 고민과 판단

기준과 판단에 대한 고민

- 라이선스 충돌에 대한 이슈
- 일반적인 소스코드에 대한 판단과 처리 문제
- 시간과 비용에 대한 고민
-
-
-

Open Your Source

E-Nable 의수 제작 지원 프로젝트



Q & A

kt ds

Thank you

kt ds