

오픈소스 통합 관리 솔루션

OBICs-COMPASS 3.0.0

2019.03

kt ds



00. 요약

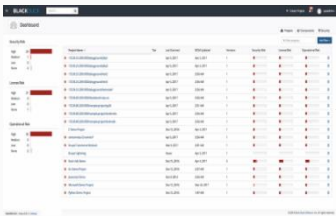
OBICs COMPASS (Open-source Compliance & Security Management Solution for Enterprise)

오픈소스 라이선스(Protex) 및 보안취약점(Hub) 통합관리

OBICs COMPASS를 통해 오픈소스에 대한 사전검토 / 검출이력관리 / 조치결과관리 / 모니터링 제공



Protex
(라이선스 검출)



Hub
(보안취약점 검출)

프로젝트 정보

홈 > 프로젝트 > 프로젝트 목록 > 프로젝트 정보

추가검검 등록

목록

프로젝트	오픈소스 프로젝트 02		
등록 상태	접수완료	PM	
배포범위	외부	특허대상	대상
구성원			
의견			

오픈소스 사전검토 요청목록

신규검토요청

오픈소스SW	버전	라이선스	보안취약점	검토상태	결과	요청일
jquery.com	1.9.1	MIT License	CVE-2018-801...	검토대기	waiting	2018-12-05

소스코드 준법성 검증이력

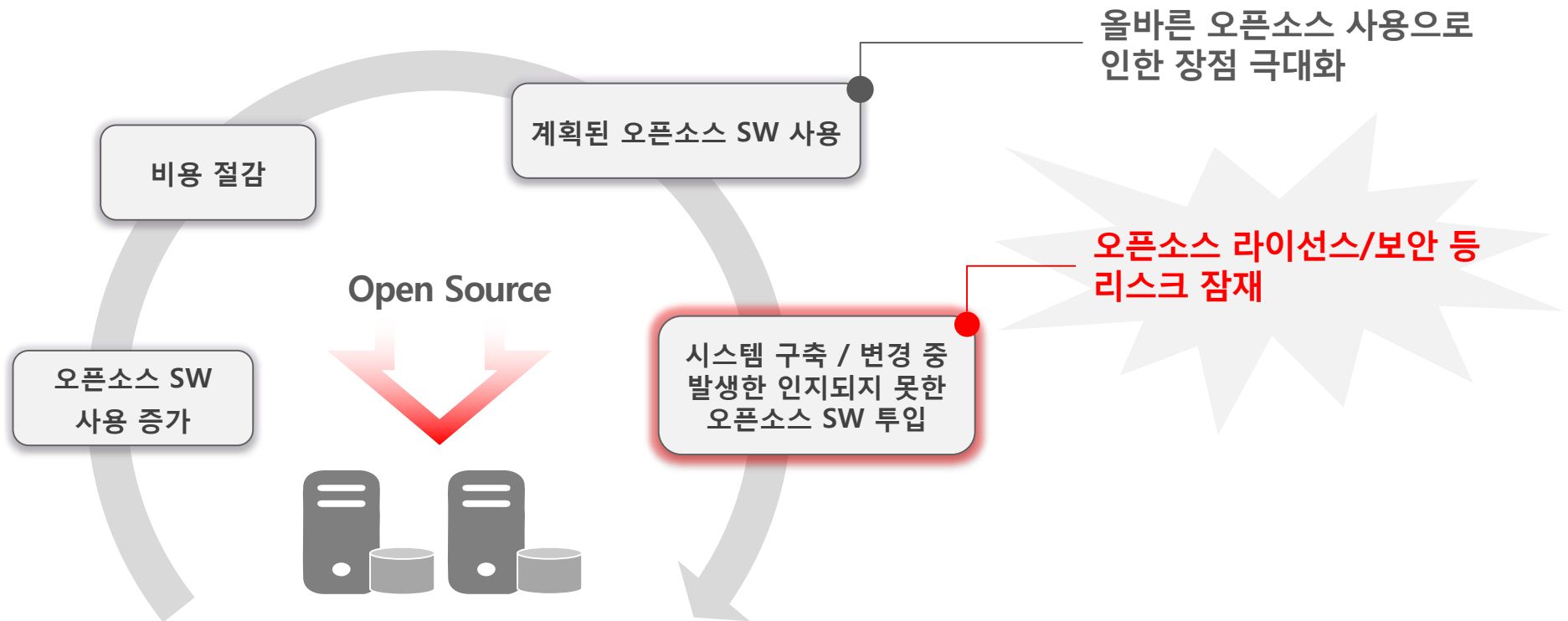
차수	요청자	요청일	검증상태	검출개수	결과	완료일
1	관리자	2018-11-08	리뷰중	4	결과	

오픈소스 보안취약점 검사이력 (※ 오픈소스 검출내역은 준법성 검증이력 검출내역과 상이할 수 있습니다.)

버전	요청자	요청일	진단상태	결과	High	Medium	Low	None	완료일
1	관리자	2018-12-11	취약점 조치	결과	0	8	0	13	

01. 기업 그리고 오픈소스

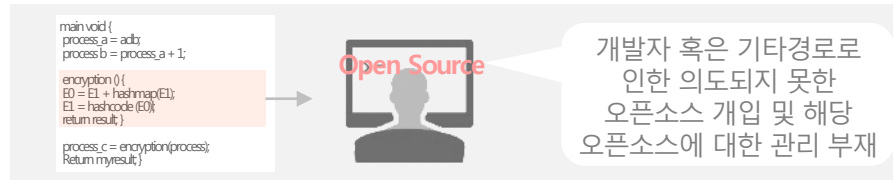
오픈소스를 올바르게 사용했을 경우 비용절감, 개발기간 단축 등 이점이 극대화되지만, 관리되지 못한 오픈소스의 사용으로 인해 라이선스 및 보안 리스크가 발생할 수 있습니다. 따라서, 기업은 지속적이고 체계적인 오픈소스 관리가 필요합니다.



01. 오픈소스 리스크 및 통합관리 필요성

다양한 케이스를 통해 오픈소스 Risk가 발생할 수 있습니다.

✓ 개발 과정에서 인지되지 못한 오픈소스가 추가되는 경우



✓ 새로운 오픈소스 보안취약점이 발견되었으나, 기업에서 해당 오픈소스SW 사용에 대해 인지하지 못하고 있는 경우



컴퓨팅 "오라클, 대규모 자바 라이선스 감사 돌입"

"오라클" 라이선스 위반했다" 연방법원 기판, 증가 추세

임민철 기자 | 입력 : 2016.12.19 18:30 | 수정 : 2016.12.20 16:30

오라클이 '자바' 사용 기업들 대상으로 대대적인 라이선스 감사(audit)에 나섰다는 외신 보도가 나와 주목된다. 규약 위반 사항을 잡거나 금전적인 배상 책임을 묻겠다는 공식 임의로 보인다. 내년엔 이를 확대할 전망이다. 국내외 자바 고객사와 파트너의 부담이 가중될 수 있다.

영국 IT미디어 더레지스터는 지난 16일 오라클이 고객사를 상대로 자바 라이선스를 위반했다고 주장하며 대대적인 감사를 벌이고 있다고 보도했다. 자바 컴플라이언스를 벗어났다는 주장을 들고 온 오라클과 접촉한 고객사와 파트너 수가 증가 추세라고 덧붙였다.

출처: <http://www.ciokorea.com>

[해킹조각크: Oracle finally targets Java non-payers? six years after]

"오픈소스 보안 취약점 이용 랜섬웨어 등장할까"

블랙햇소프트웨어 "오픈소스 보안 취약점 관리 제대로 안돼-랜섬웨어APT 공격 증가할 것"

2017년 08월 21일 18:26:36 | 김선영 기자 | lyammi@datanet.co.kr

워너크라이에 이어 웹 호스팅 기업 인터넷N에나 랜섬웨어 피해까지 발생하면서 랜섬웨어는 전 세계의 공표가 되고 있다. 이와 함께 오픈소스 취약점을 악용한 랜섬웨어 공격이 발생한다면, '보안 사고의 새로운 역사'를 쓰게 될 것이라는 경고도 나온다.

이미 오픈소스를 악용하는 랜섬웨어가 발효된 바 있다. 랜섬웨어 공격 방식과 위험도 등을 가르치기 위해 오픈소스로 개발된 코드를 악용한 '매직(Magic)' 랜섬웨어가 지난해 발견된 바 있다.

블랙햇소프트웨어가 5월 발표한 보고서 '2017 OSSRA(Open Source Security & Risk Analysis)'에 따르면 96%의 애플리케이션이 오픈소스를 사용하고 있으며, 67%는 취약점이 있는 오픈소스를 사용하고 있다. 금융산업에서는 앱 당 52개의 취약점을 보유하고 있으며, 80%는 고위험 취약점을 내포하고 있다. 리테일과 이커머스 부문 무료 83%가 높은 위험의 보안 취약점이 있다.

김병선 블랙햇소프트웨어코리아 상무는 "거의 모든 산업군에서 오픈소스가 사용되고 있으며, 거의 대부분의 오픈소스는 보안 취약점을 갖고 있다. 이 취약점이 해결되지 않으면 심각한 보안위험에 직면할 수 있으며, 랜섬웨어와 같이 직접적인 금전 피해와 비즈니스 중단 상황을 겪게 될 수도 있다"고 말했다.

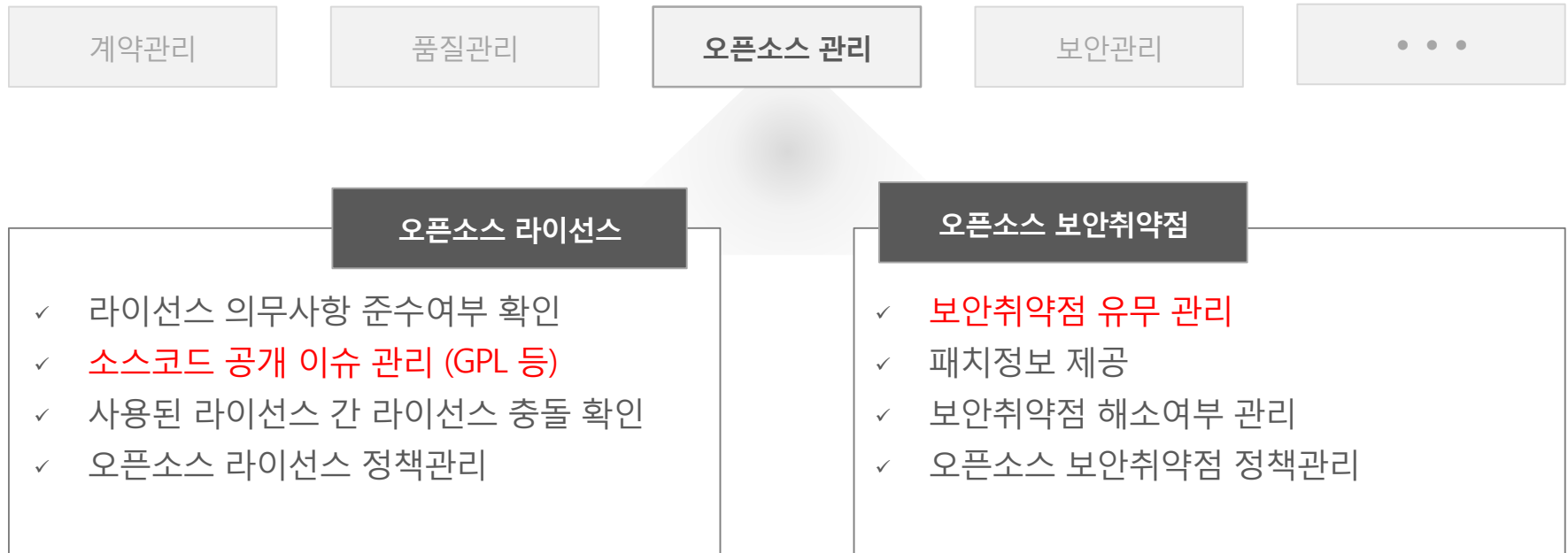
[관련기사: '공통' 오라클, 천마이크로시]
[관련기사: '천 인수로 5년내 매출 두배'
[관련기사: EC, 오라클-천 합병승인]
[관련기사: 조나단 슈워츠 천 CEO가 적다]

이후 오라클은 자바를 활용해 다각도로 수익화 방안을 모색해

01. 오픈소스 리스크 및 통합관리 필요성

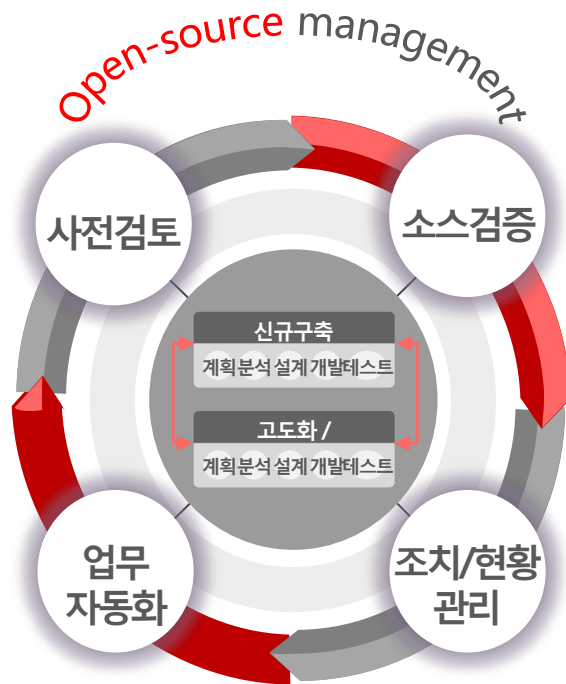
사용자 입장에서 오픈소스 라이선스와 보안취약점에 대한 관리, 조치, 문의 등에 대한 채널을 일원화하고, 오픈소스 라이선스/보안취약점 각 분야의 담당자가 하나의 시스템에서 상호 이슈 확인이 가능하기 위해 통합관리가 필요합니다.

PROJECT MANAGEMENT



- OSS 보안취약점을 포함한 시스템 소스를 라이선스에 의해 공개 해야하는 경우 발생 > 기업 이미지 손실방지
- 사용자 입장에서 오픈소스 라이선스 / 보안취약점 간 이중 관리채널 > 사용자 불편함 해소

02. OBICs COMPASS 소개



What

오픈소스 사용 가이드라인을 제공하고 개발 SW에 인용된 오픈소스의 저작권 침해와 라이선스 위반, 보안취약점을 관리함으로써 리스크를 미연에 방지하며, 체계적인 오픈소스 통합관리 기능을 제공합니다.

Why

- 1 사전 계획과 다르게 사용된 오픈소스에 대한 검출 필요
- 2 오픈소스 사용에 대한 라이선스/보안 이슈 사전방지
- 3 오픈소스 관리 체계구축의 밑바탕

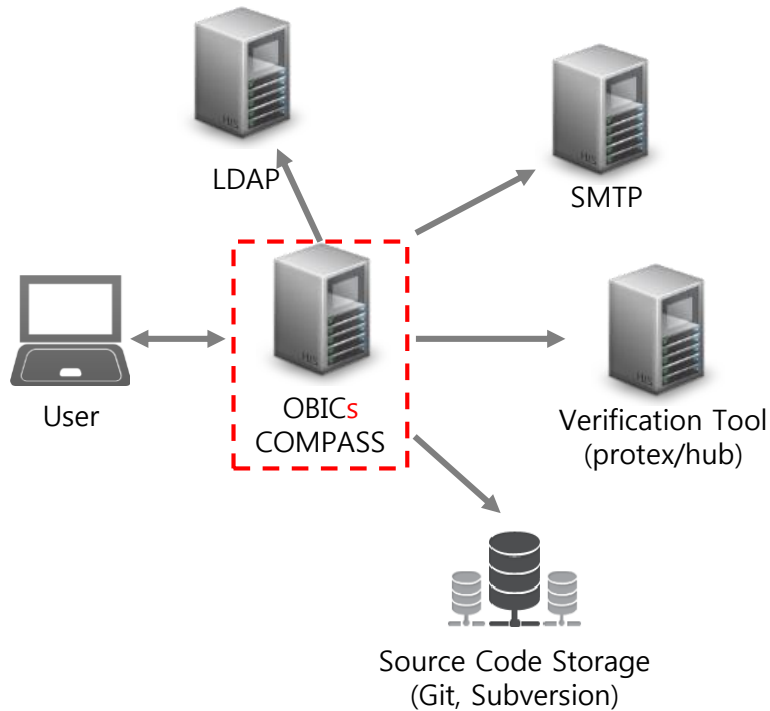
Who



03. OBICs COMPASS 구성

OBICs COMPASS는 오픈소스 라이선스 검증툴 Protex, 오픈소스 보안취약점 검증툴 Hub와 연동하며, Web 형태로 사용자에게 제공됩니다.

Overview



Advantages



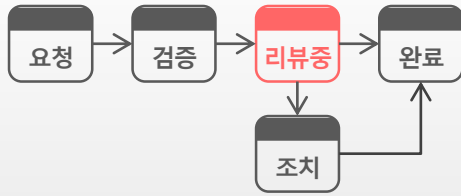
Workflow 기반 오픈소스 End-to-End 관리

자동 레포트 생성 및 다운로드

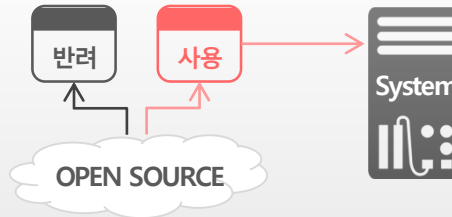
오픈소스 현황 실시간 모니터링

오픈소스 SW 정보 검색

04. OBICs COMPASS 주요기능 (ver. 3.0.0 기준)



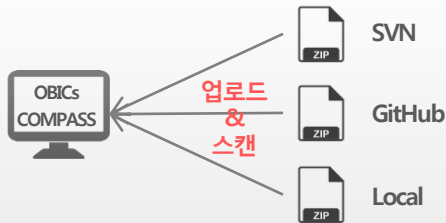
오픈소스 관리 프로세스화



오픈소스 사전검토



실시간 오픈소스 모니터링



소스코드 업로드 채널



자사 오픈소스 DB 구축

OSS Repository

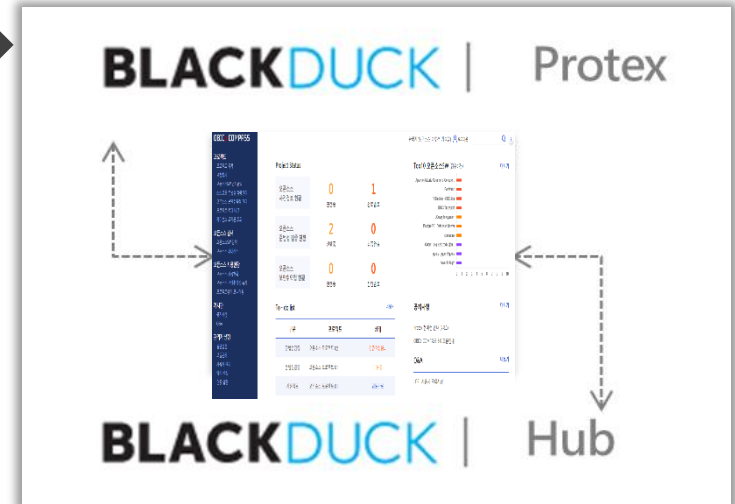


기타 유틸리티

05. OBICs COMPASS 특징점

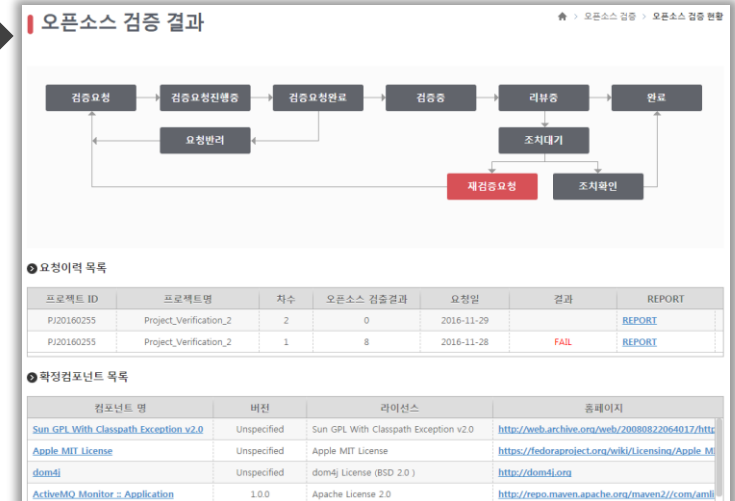
국/내외 최대 오픈소스 라이선스/보안 솔루션과의 연동 및 관리

- 국내/외 최대 오픈소스 메타데이터를 보유하는 Protex와 연동하여 관리 채널을 제공합니다.
- 오픈소스 보안취약점 최대 데이터를 보유하는 Hub와 연동하여 관리 채널을 제공합니다.



기업 검증 관리 노하우로 구축된 검증 프로세스

- 약 1000건 이상의 검증 및 관리 노하우를 바탕으로 정립된 프로세스를 제공합니다.
- 체계적인 프로세스로 오픈소스 관리 사각지대를 해소합니다.
- 검증 관리 프로세스를 도입함으로써 검증 툴의 도입 효과를 극대화합니다.



05. OBICs COMPASS 특징점

오픈소스 사전 검토를 통한 프로젝트 비용절감 효과

- 잘못된 오픈소스 사용으로 개발완료 후 제거/수정으로 인해 발생하는 리소스, 즉 추가 비용 발생을 예방하고 절감할 수 있습니다.
- 시스템 도입 시, 효율적인 검토 체계를 수립할 수 있습니다.
- 오픈소스 사전검토를 통해 올바른 오픈소스 정보를 전달합니다.

오픈소스SW 검색

apache commons 검색

상세검색 ☐ GPL ☐ LGPL ☒ Apache ☐ MIT ☐ BSD

20 [상세버전]을 클릭하여 내 프로젝트에

오픈소스 SW	버전	대표 라이선스
99soft :: SL4J :: Apache Commons Logging	상세버전	Apache License 2.0
Apache Commons DBCP JMX extensions :: JDBC4	상세버전	Apache License 2.0
Apache Stanbol Commons Namespace Prefix Provider for Stan	상세버전	Apache License 2.0
Apache Sling Commons Java Compiler	상세버전	Apache License 2.0
Apache Oltu - Commons - Encoded Token	상세버전	Apache License 2.0
KIE EAP - org-apache-commons-vfs static module	상세버전	Apache License 2.0
Apache Jakarta Commons Clazz	상세버전	Apache License 2.0

실시간 현황 통계 및 오픈소스 사용 정보 모니터링

- 기업에서 사용되고 있는 오픈소스 현황을 실시간으로 수집 및 모니터링이 가능합니다.
- 오픈소스 보안취약점 최대 데이터를 보유하는 Hub와 연동하여 관리 채널을 제공합니다.
- 오픈소스 이슈 발생 시, 즉각적 확인 및 대처가 가능합니다.



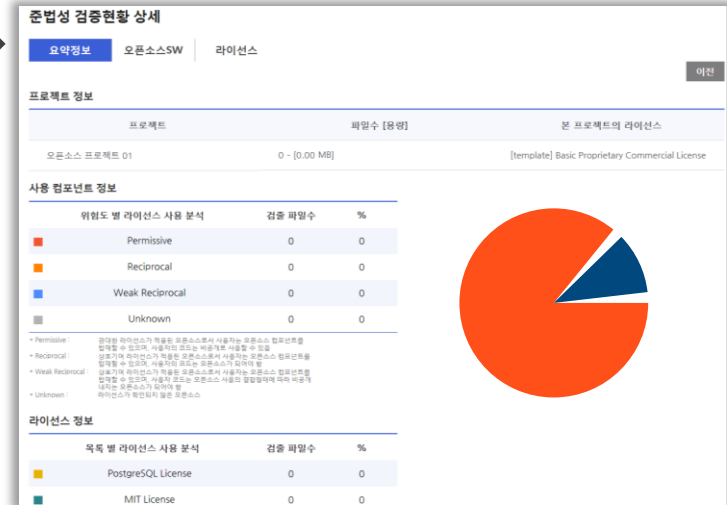
05. OBICs COMPASS 특징점

관리에 필요한 기능 자동화 및 관리 효율성 증대

- 관리 시 필요한 수동적인 부분들을 자동화하여 전사의 시스템을 효율적으로 관리할 수 있습니다.
- 결과 보고서 자동 생성 / 오픈소스 고지문 자동 생성 / Alert 기능 / 프로젝트 오픈소스 결과 비교 / 이력 관리 등

기업 내 오픈소스 통합 채널 제공

- 형상관리 툴과의 연동 등을 통해 손쉬운 소스코드 업로드 기능을 제공합니다.
- 통합된 올바른 오픈소스 정보를 제공합니다. (오픈소스 검색, 블랙덕에서 제공하는 오픈소스 라이선스 풀이정보 등).
- 한글화 등 사용자 친화적인 화면을 통해 기업 구성원 누구든지 오픈소스에 대해 쉽게 접근할 수 있도록 합니다.



라이선스 상세

Apache License 2.0

라이선스(원문)

의무사항 표

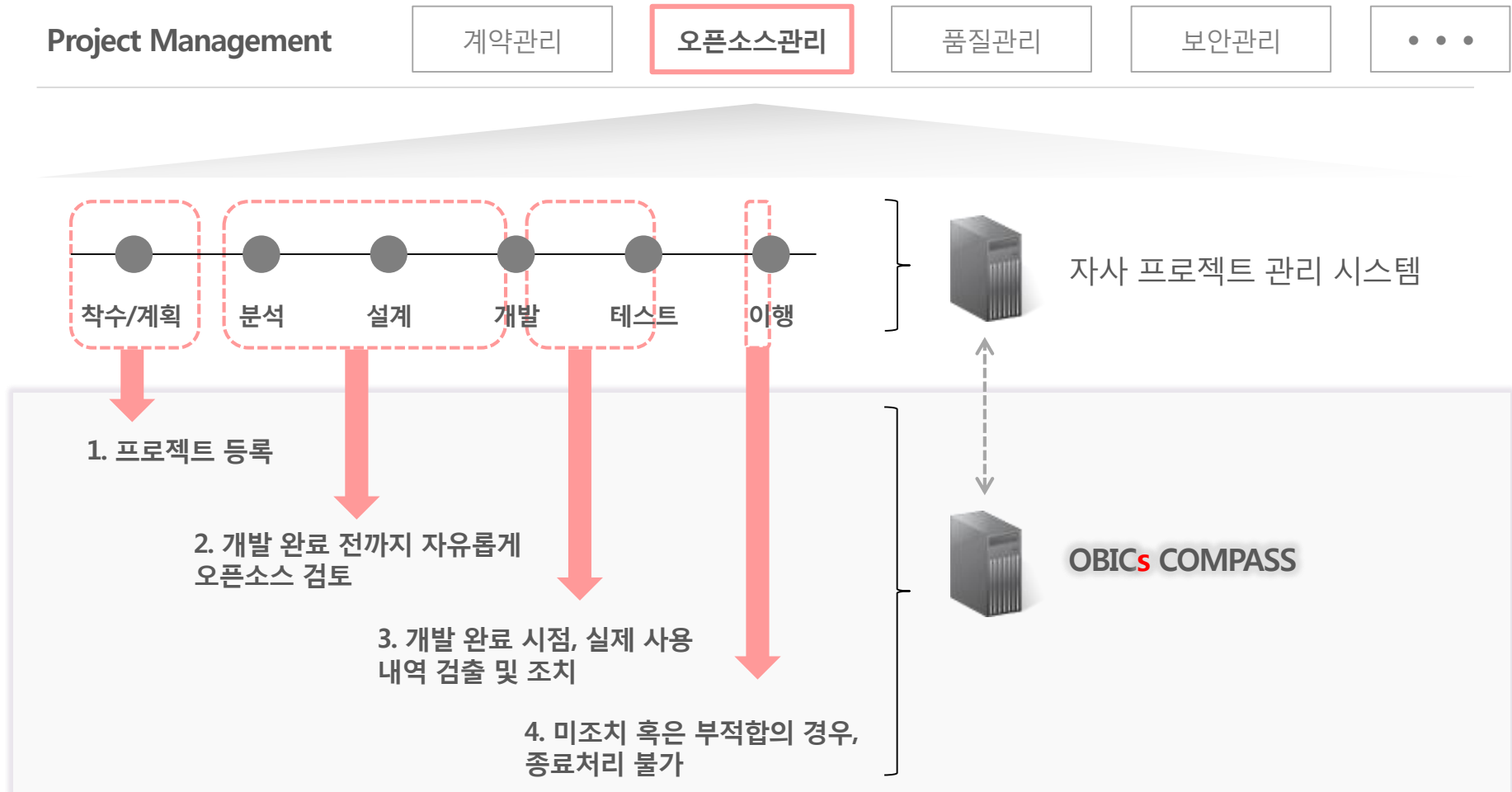
의무사항	결과
1. 배포권리	○
2. 배포 (코드배포에 의해서만 부여되는 의무사항)	X
3. 소스코드 배포/ 강제적 공유 의무사항	△
4. 복제권한 허용	△
5. 수정/개작권한 허용	△
6. 역설계 권한 허용	△
7. 차별적 제한조건	△

3. 소스코드 배포/ 강제적 공유 의무사항

- : 다른 사용자에게 소스코드를 의무적으로 공개해야 합니다.
- △ : 다른 사용자에게 해당 소스코드를 공개해도 되고, 하지 않아도 됩니다.
- X : 다른 사용자에게 해당 소스코드를 공개할 수 없습니다.

06. OBICs COMPASS 적용사례

솔루션 적용 사례의 경우, 기존 자사 프로젝트 관리 시스템과 연동하여 체계적인 오픈소스 관리 프로세스를 추가 적용하고 있습니다.



별첨 Protex – 오픈소스 라이선스 검출

Protex는 전 세계적으로 최대 오픈소스 메타데이터(Knowledge-Base)를 보유하고 있으며, 이 메타데이터를 기반으로 소스코드 라인 레벨의 정밀한 오픈소스 스캔 및 라이선스 검출을 수행합니다.

BLACKDUCK | Protex

dev@kt.com

[Tools](#) [Help](#) [Logout](#)

Server: protex.blackducksoftware.co.kr

Server Version: 7.7.1

My Protex Manage Identify Review Report

Current Project: fdf_PJ20170040_1

Project Status:

2,830 0 0 0 0 0 468

Show: Pending Identification - ALL

New Filter...

Expand Collapse

☐ Only Show Matches

Clear

fdf_PJ20170040_1 (2,830)

bin (1,702)

product (1,039)

apps (1,039)

Catalina (534)

ROOT (534)

css (4)

fonts

images

jqplot (2)

jquery.js

jquery.js

js (1)

zTreeStyle

bootstrap.css

common.css

common2.css

contents.css

layout.css

Bill of Materials

Code Matches

Searches

Dependencies

Rapid ID

Teach IDs

History

+	KB	Intro.js	8	Unspecified	GNU Affero General Public License v3.0 (and others)	September 01, 2016	File	Precision Match	100	intro.js-v2.5.0.tar.gz/intro.2.5.0/example/bootstrap/v
+	KB	AdminLTE	7	Unspecified	MIT License	November 04, 2016	File	Precision Match	100	AdminLTE-v2.3.10.tar.gz/A
+	KB	Bootstrap - org.webjars:bootstrap	5	Unspecified	Apache License 2.0	July 25, 2016	File	Precision Match	100	bootstrap-3.3.7-1.jar/MET/
	KB	Bootstrap	9	3.3.7	MIT License	July 25, 2016	File	Precision Match	100	bootstrap-v3.3.7.tar.gz/bo
	KB	bootswatch	9	3.3.7	MIT License	July 30, 2016	File	Precision Match	100	bootswatch-3.3.7.tar.gz/bc
+	KB	Bootstrap-Admin-Template	7	Unspecified	MIT License	July 31, 2016	File	Precision Match	100	Bootstrap-Admin-Template-2.4.2/public/ass

Your File: bootstrap.css

```
1. /*!  
2. * Bootstrap v3.3.7 (http://getbootstrap.com)  
3. * Copyright 2011-2016 Twitter, Inc.  
4. * Licensed under MIT (https://github.com/twbs/boot  
5. */  
6. /*! normalize.css v3.0.3 | MIT License | github.com  
7. html {  
8.   font-family: sans-serif;  
9.   -webkit-text-size-adjust: 100%;  
10.  -ms-text-size-adjust: 100%;
```

Matched File: bootstrap.css

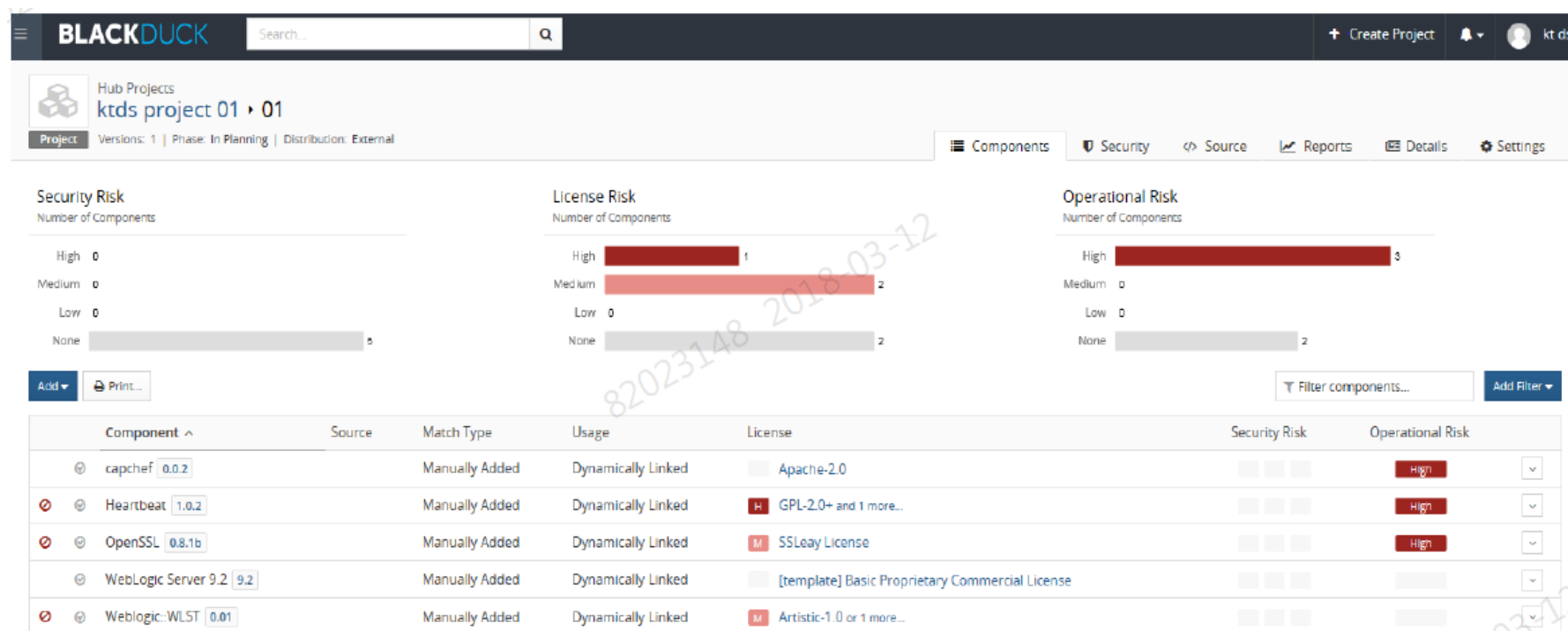
```
1. /*!  
2. * Bootstrap v3.3.7 (http://getbootstrap.com)  
3. * Copyright 2011-2016 Twitter, Inc.  
4. * Licensed under MIT (https://github.com/twbs/boot  
5. */  
6. /*! normalize.css v3.0.3 | MIT License | github.com/n  
7. html {  
8.   font-family: sans-serif;  
9.   -webkit-text-size-adjust: 100%;  
10.  -ms-text-size-adjust: 100%;
```

>> 시스템 Source Code

>> Protex Knowledge Base

별첨 HUB – 오픈소스 보안취약점 검출

Hub는 전세계적으로 최대 오픈소스 보안취약점 메타데이터를 보유하고 있으며, 이 메타데이터를 기반으로 소스트리 스캔을 수행하여 오픈소스 보안취약점을 검출합니다.



Displaying 1-5 of 5

별첨 주요기능(1/6)



오픈소스 사용에 대한 후속 관리가 중요합니다. 이를 시스템으로 프로세스화 함으로써 체계적인 관리 및 안전한 오픈소스 사용이 가능합니다.

별첨 주요기능(2/6)

오픈소스 관리 프로세스화

오픈소스 사전검토

실시간 오픈소스 모니터링

소스코드 업로드 채널

OSS Repository

기타 유틸리티

오픈소스 검색

오픈소스SW 검색

apache commons 검색

상세검색 ☐ GPL ☐ LGPL ☒ Apache ☐ MIT ☐ BSD

20 [상세버전]을 클릭하여 내 프로젝트에 ,

오픈소스 SW	버전	대표 라이선스
99soft :: SL4J :: Apache Commons Logging	상세버전	Apache License 2.0
Apache Commons DBCP JMX extensions :: JDBC4	상세버전	Apache License 2.0
Apache Stanbol Commons Namespace Prefix Provider for Stanb	상세버전	Apache License 2.0
Apache Sling Commons Java Compiler	상세버전	Apache License 2.0

임시저장에 검토목록 담기

현재 목록보기

● 임시저장 컴포넌트 목록

컴포넌트명	버전	라이선스
hahaha	Generic Version	ISC License
App-OracleInfo	Generic Version	Unspecified
knife-oracle_public_cloud	Generic Version	Apache License 2.0
knife-oracle_public_cloud	0.0.5	Apache License 2.0

검토완료

● 오픈소스 컴포넌트 검토이력


컴포넌트명	버전	라이선스	검토상태	사용승인결과
shhtpd	Generic Version	Unspecified	검토완료	Y
shhtpd	Generic Version	Unspecified	검토완료	N
httpd_ctl	1.00	GNU General ...	검토완료	Y
jboss-javac	5.0.2.GA	Unspecified	검토완료	Y
jboss-javac	5.0.1.GA	Unspecified	검토완료	Y

검토요청

오픈소스 컴포넌트 사용 승인 요청 내역

프로젝트 ID	프로젝트명	등록 상태	요청일
P/20170027	test2	검토대기	2017-05-25

담당자 검토



Confirm

Reject

설계 혹은 개발 초기 단계에서 **사전에 오픈소스 사용에 대해 검토함**으로써 추후 오픈소스로 인한 **라이선스/보안 이슈로 인한 추가개발을 사전 방지**합니다. 따라서 비용절감 효과를 기대할 수 있습니다.

별첨 주요기능(3/6)

오픈소스 관리 프로세스화

오픈소스 사전검토

실시간 오픈소스 모니터링

소스코드 업로드 채널

OSS Repository

기타 유틸리티



관리자는 **프로젝트 관리상태**, **오픈소스 사용 통계**, **보안취약점 통계**에 대한 정보를 실시간으로 조회하여 **모니터링**할 수 있습니다. 따라서, 오픈소스로 인한 이슈 발생 시, 즉각 적인 대응이 가능합니다.

별첨 주요기능(4/6)

오픈소스 관리 프로세스화

오픈소스 사전검토

실시간 오픈소스 모니터링

소스코드 업로드 채널

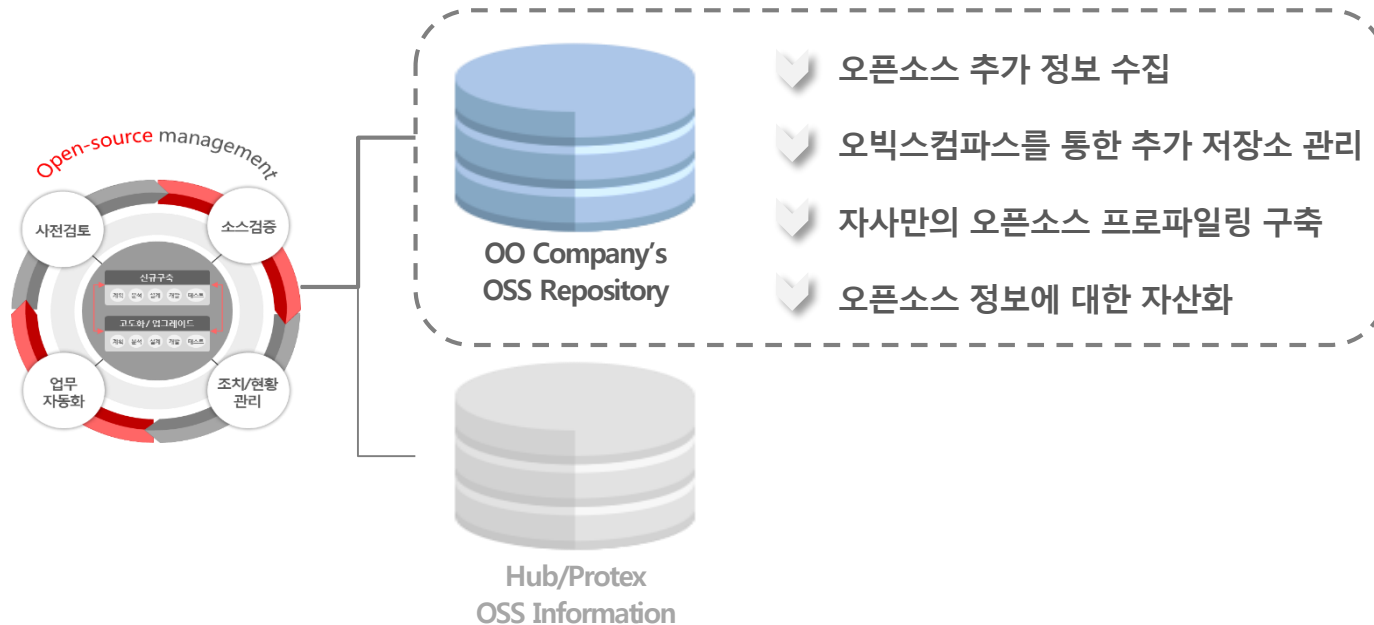
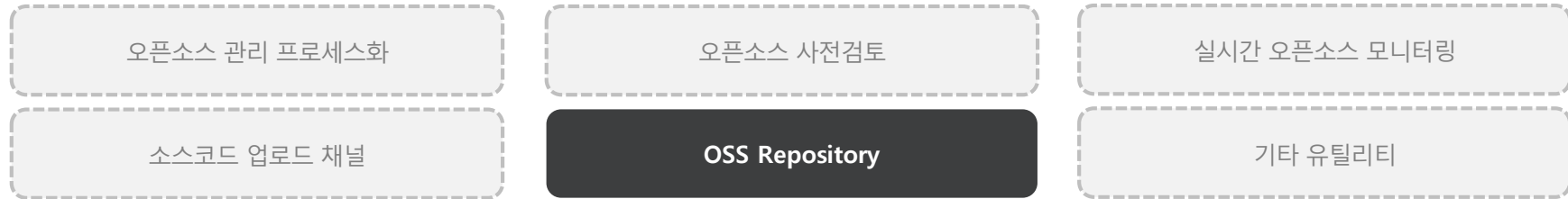
OSS Repository

기타 유틸리티



사내 누구나 접근 가능한 Web 형태로 제공되어 손쉽게 검증하고자 하는 소스코드를 업로드할 수 있으며, 형상관리 시스템과도 연계하여 자동 업로드가 가능합니다.

별첨 주요기능(5/6)



OSS Repository는 자사만의 오픈소스 메타데이터 정보를 구축하며, OBICs COMPASS를 통해 손쉽게 관리하고 기업 내 구성원이 상세하게 프로파일링 된 오픈소스 정보를 조회할 수 있습니다.

별첨 주요기능(6/6)

오픈소스 관리 프로세스화

소스코드 업로드 채널

오픈소스 사전검토

OSS Repository

실시간 오픈소스 모니터링

기타 유틸리티

라이선스 고지문 조회

오픈소스 프로젝트 01_1

오픈소스 프로젝트 > 라이선스 고지문 조회

추가 미리보기 HTML 다운로드

오픈소스SW	버전	라이선스	URL	Copyright	선택
Apache Jakarta Commons Co...	0.1-dev	Apache License 2.0	http://jakarta.apache.org/co...		선택
Bootstrap	Unspecified	MIT License	http://getbootstrap.com		선택
commons	Unspecified	Apache License 2.0	http://github.com/twitter/co...		선택
CKEditor - CKEditor	Unspecified	GNU General Public...	http://www.ckeditor.com		선택
JDBC Transport	Unspecified	Common Public Attri...	http://www.mulesoft.org/mul...		선택
jQuery - org.jscip.redisquery	2.0.1	MIT License	http://jscip.org/redisquery		선택
jquery - jquery/jquery	1.0a	MIT License	http://github.com/jquery/jqu...		선택
jQuery Integration	Unspecified	Apache License 2.0	http://mirrors.ibiblio.org/max...		선택
naver-id-login	Unspecified	ISC License	https://www.npmjs.org/packa...		선택
PostgreSQL Database Server	Unspecified	PostgreSQL License	http://github.com/postgres/p...		선택

프로젝트 결과 비교

오픈소스 프로젝트 01_1

오픈소스 SW 수 (공통: 10건, 추가: 0건, 선택: 0건)

오픈소스 프로젝트 01_1

오픈소스SW	버전	라이선스	URL	오픈소스SW	버전	라이선스	URL
Apache Jakarta Co...	0.1-dev	Apache Licen...	http://jakarta.apac...	Apache Jakarta Co...	0.1-dev	Apache Licen...	http://jakarta.apac...
Bootstrap	Unspecified	MIT License	http://getbootstrap...	Bootstrap	Unspecified	MIT License	http://getbootstrap...
commons	Unspecified	Apache Licen...	http://github.com...	commons	Unspecified	Apache Licen...	http://github.com...
CKEditor - CKEditor	Unspecified	GNU General...	http://www.ckedit...	CKEditor - CKEditor	Unspecified	GNU General...	http://www.ckedit...
JDBC Transport	Unspecified	Common Pub...	http://www.mules...	JDBC Transport	Unspecified	Common Pub...	http://www.mules...
jQuery - org.jscipr...	2.0.1	MIT License	http://jscip.org/re...	jQuery - org.jscipr...	2.0.1	MIT License	http://jscip.org/re...
jquery - jquery/jqu...	1.0a	MIT License	http://github.com...	jquery - jquery/jqu...	1.0a	MIT License	http://github.com...
jQuery Integration	Unspecified	Apache Licen...	http://mirrors.ibib...	jQuery Integration	Unspecified	Apache Licen...	http://mirrors.ibib...
naver-id-login	Unspecified	ISC License	https://www.npmj...	naver-id-login	Unspecified	ISC License	https://www.npmj...
PostgreSQL Databa...	Unspecified	PostgreSQL Li...	http://github.com...	PostgreSQL Databa...	Unspecified	PostgreSQL Li...	http://github.com...

오픈소스 프로젝트 > 프로젝트 결과 비교

오픈소스 검증 현황

오픈소스 프로젝트 > 오픈소스 검증 현황

프로젝트 정보

프로젝트	오픈소스 프로젝트 01	채수	1
요청자	관리자	요청일	2018-11-06
설명	검증 부탁드립니다		
오픈소스 검증개수	10		

검출된 오픈소스SW 목록

오픈소스SW	버전	라이선스	출처
Apache Jakarta Commons Compress	0.1-dev	Apache License 2.0	http://jakarta.apache.org/commons/sans...
Bootstrap	Unspecified	MIT License	http://getbootstrap.com
commons	Unspecified	Apache License 2.0	http://github.com/twitter/commons/
CKEditor - CKEditor	Unspecified	GNU General Public License v2.0 or later	http://www.ckeditor.com
JDBC Transport	Unspecified	Common Public Attribution License 1.0	http://www.mulesoft.org/mule-transport



오픈소스 관리에 필요한 기능들을 자동화하여 운영 효율성이 높아질 수 있습니다.
(오픈소스 라이선스 고지문 자동생성, 오픈소스 검증 결과 프로젝트 별 비교, 자동 레포트 생성 등)

Thank you

