OpenChain-KWG 2024년 3사분기 회의

ETRI 오픈소스 거버넌스 소개

ETRI Open Source Governance

2024. 9. 10. (화)

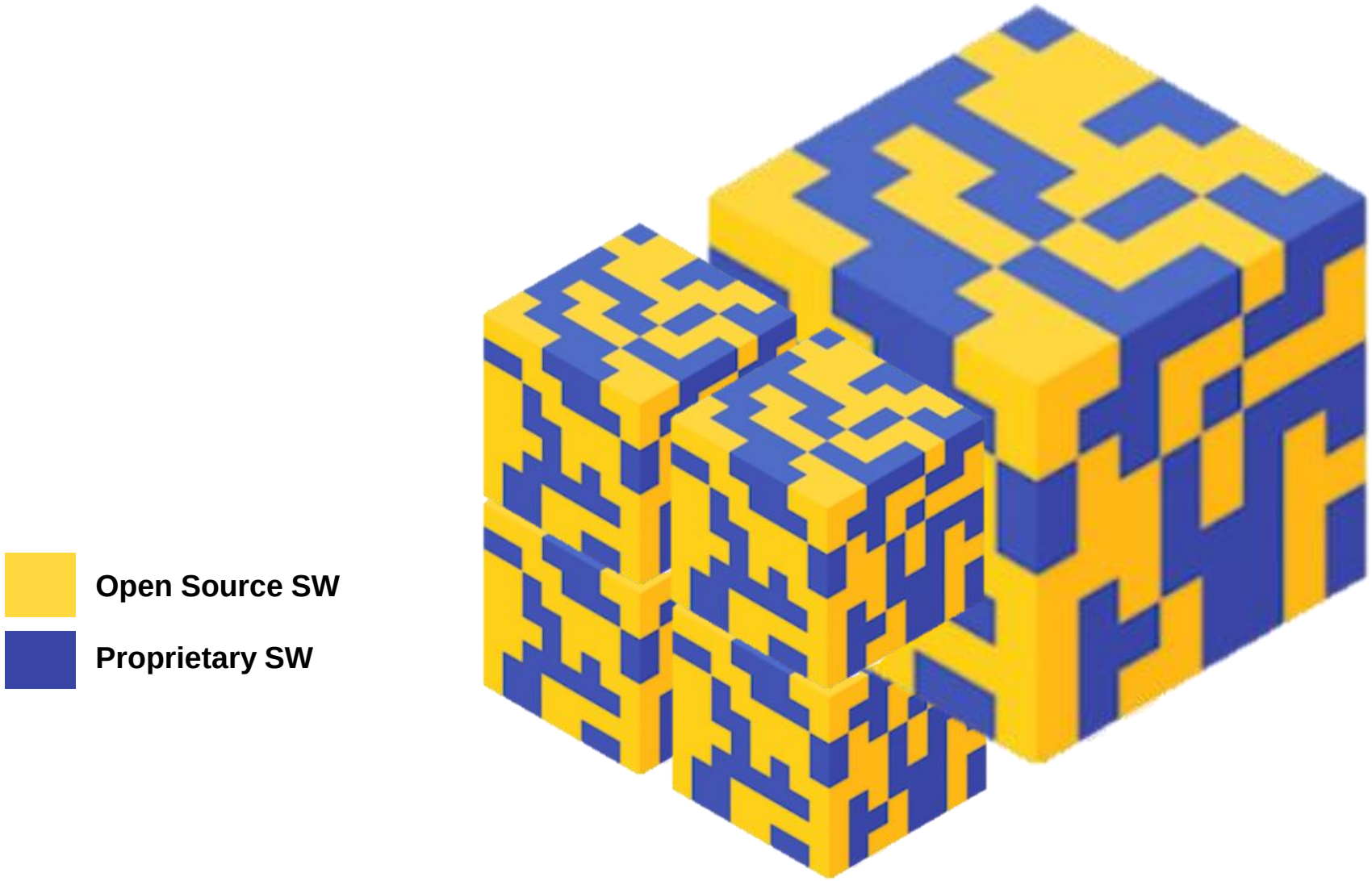
ETRI 오픈소스센터
박 정 숙

CONTENTS

01

오픈소스 리스크

요즘의 소프트웨어



오픈소스

- 오픈소스 패러다임 확산에 따라 4차 산업혁명을 견인하는 기술에도 오픈소스 비중 증가(블록체인, 클라우드, IoT, 6G 네트워크, AI 등)

출처: https://www.yonhapnewstv.co.kr/news/MYH20230213016200641

오픈소스 리스크

- **오픈소스는 라이선스 의무사항 준수없이 소스코드를 사용하여 법적인 이슈 발생 가능**
- **특히 소스코드가 공개되어 있어 보안 공격의 주 타깃이 될 수 있음**

77%

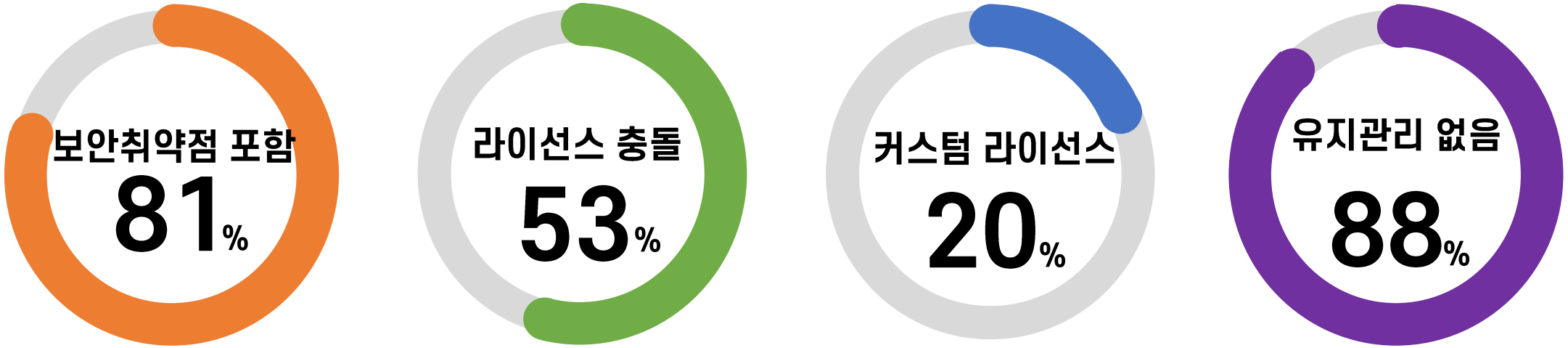
국내 50인 이상 기업 오픈소스 활용 비중
('2021 오픈소스SW(OSS) 실태조사 보고서')

97%

북미 개발 SW의 오픈소스 활용 비중
(2022, Synopsys)

80%

오픈소스 80%가 보안에 취약한 버전
(2022, Synopsys)



<출처: 2022 Open Source Security And Risk Analysis Report, Synopsis>

오픈소스 위험성 원인 분석

1. 알려진 취약점
OSS-RISK-1
Known Vulnerabilities

2. 합법 패키지 손상
OSS-RISK-2
Compromise of Legitimate Package

3. 이름 혼동 공격
OSS-RISK-3
Name Confusion Attacks

4. 미 관리
OSS-RISK-4
Unmaintained Software

5. 구 버전
OSS-RISK-5
Outdated Software

6. 추적불가
OSS-RISK-6
Untracked Dependencies

7. 라이선스 위험
OSS-RISK-7
License and Regulatory Risk

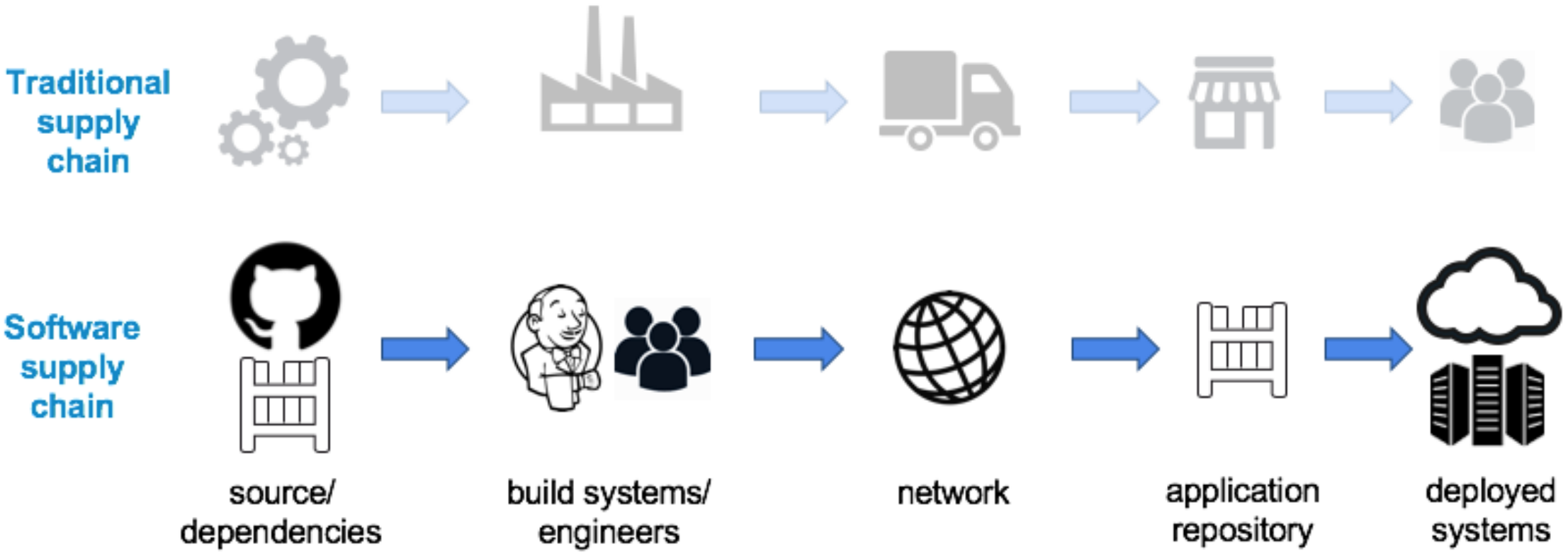
8. 미성숙성
OSS-RISK-8
Immature Software

9. 미승인 변경
OSS-RISK-9
Unapproved Change (mutable)

10. 종속성 과도/부재
OSS-RISK-10
Under/over-sized Dependency

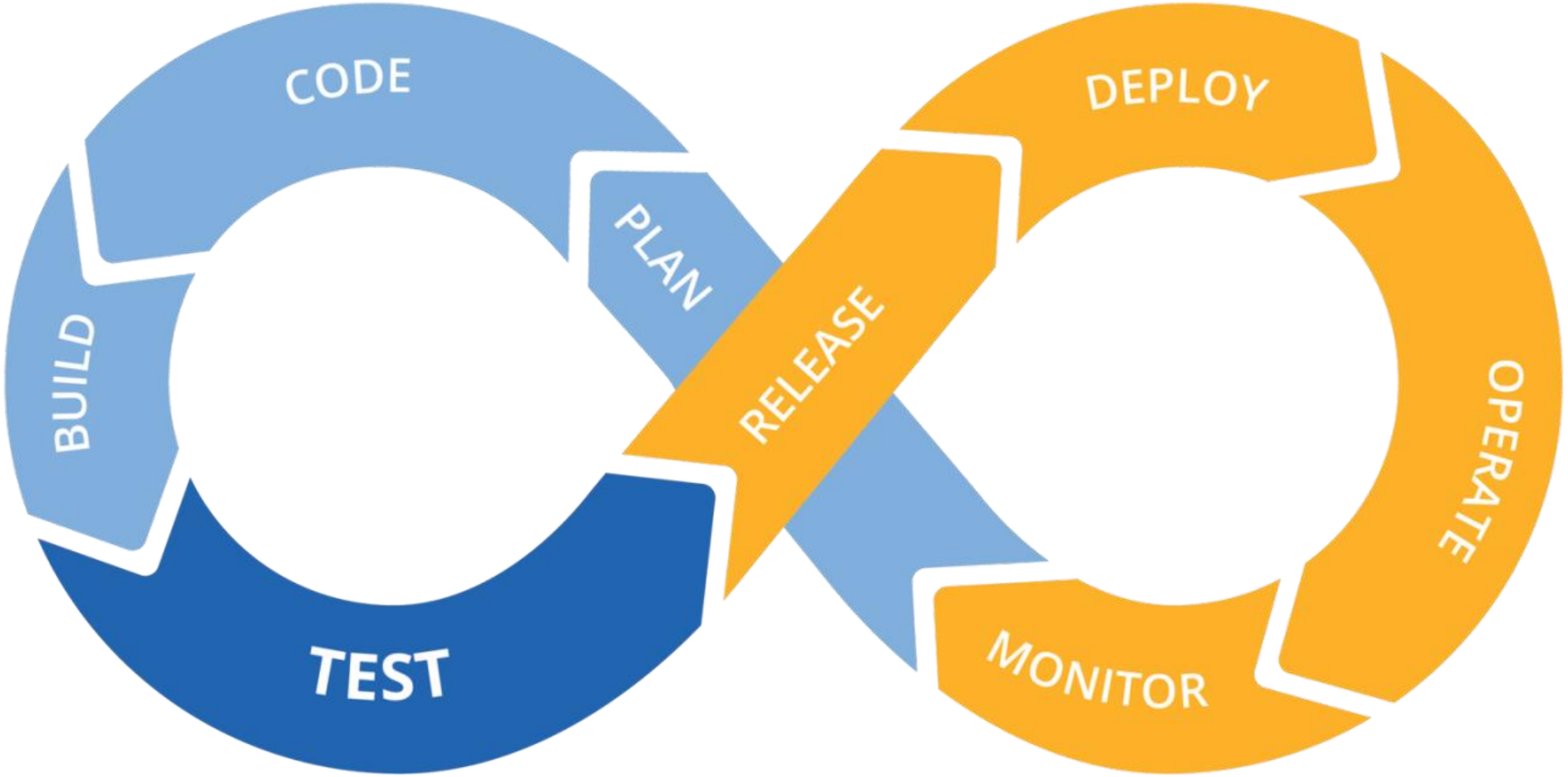
https://www.endorlabs.com/resources-overview?tab=reports-tab

SW 공급망

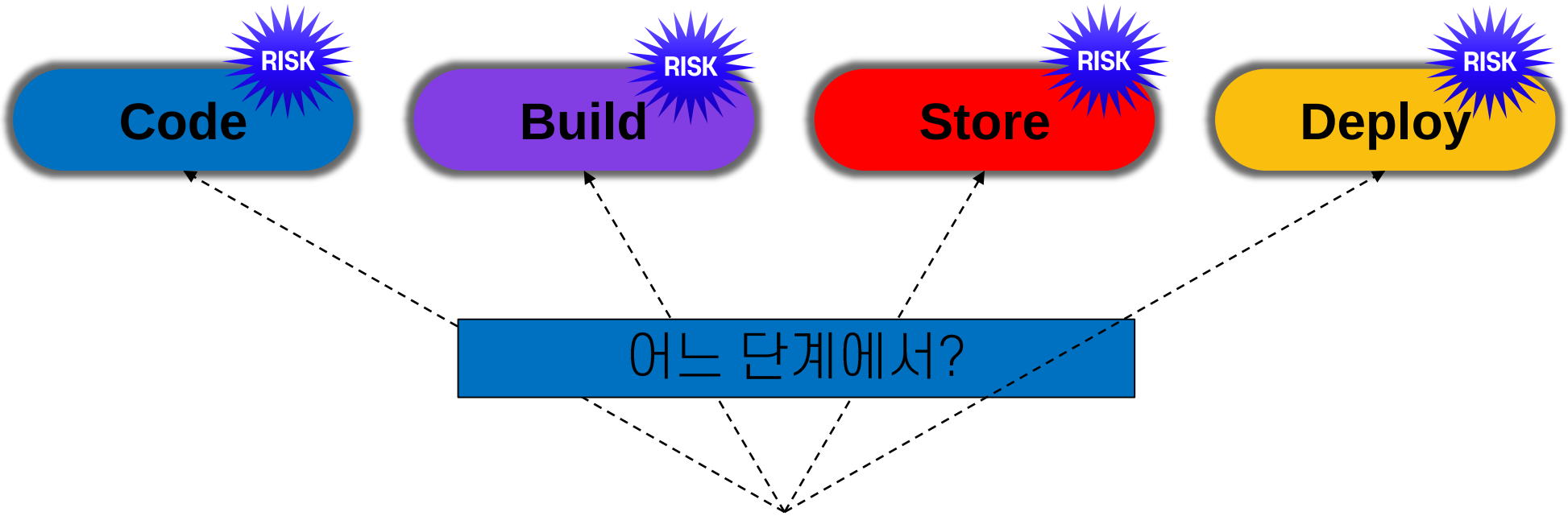


https://jenkins-x.io/blog/2022/07/24/intro-to-sbom/

SW 개발 및 배포 관점에서의 공급망

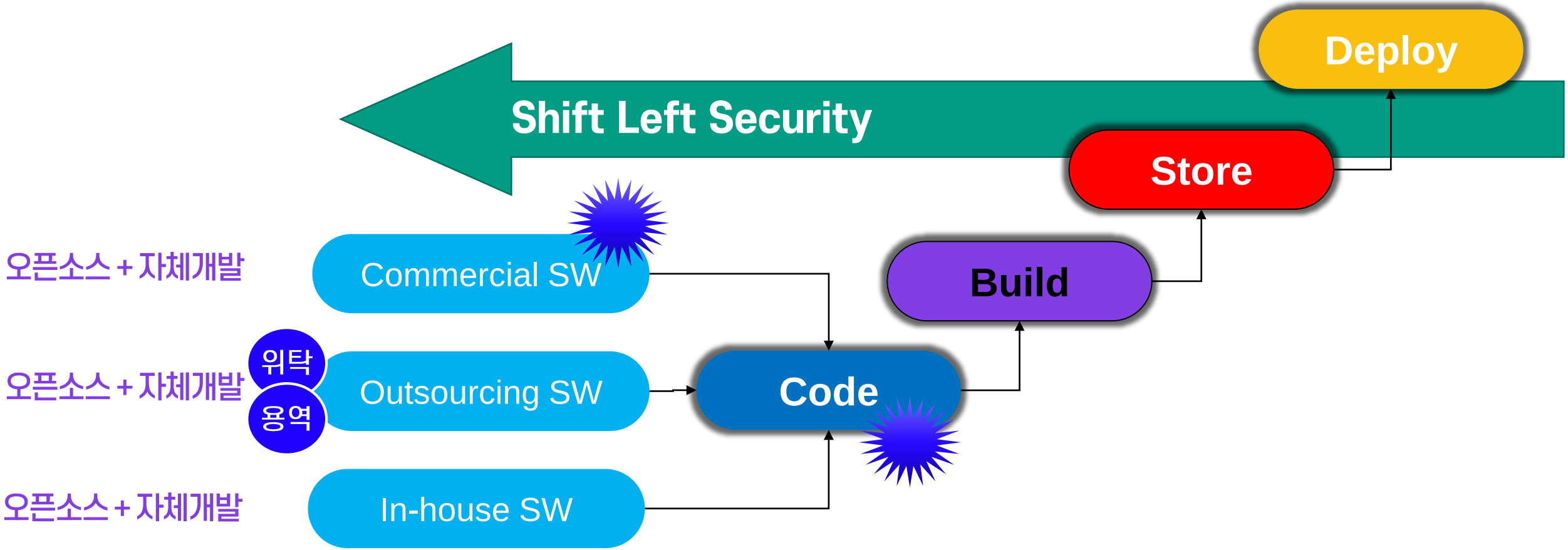


보안 관점에서 소프트웨어 공급망 관리



- 오픈소스 라이선스 검증
- 보안취약점 검사

보안 관점에서 소프트웨어 공급망 관리



02

ETRI 오픈소스 거버넌스

ETRI, OpenChain 준수 선언 | ’21.12

OPENCHAIN

ISO

THE LINUX FOUNDATION

ISO/IEC 5230 국제표준 인증기관
오픈소스 컴플라이언스 표준 인증

ETRI 오픈소스 거버넌스 체계 우수성 입증

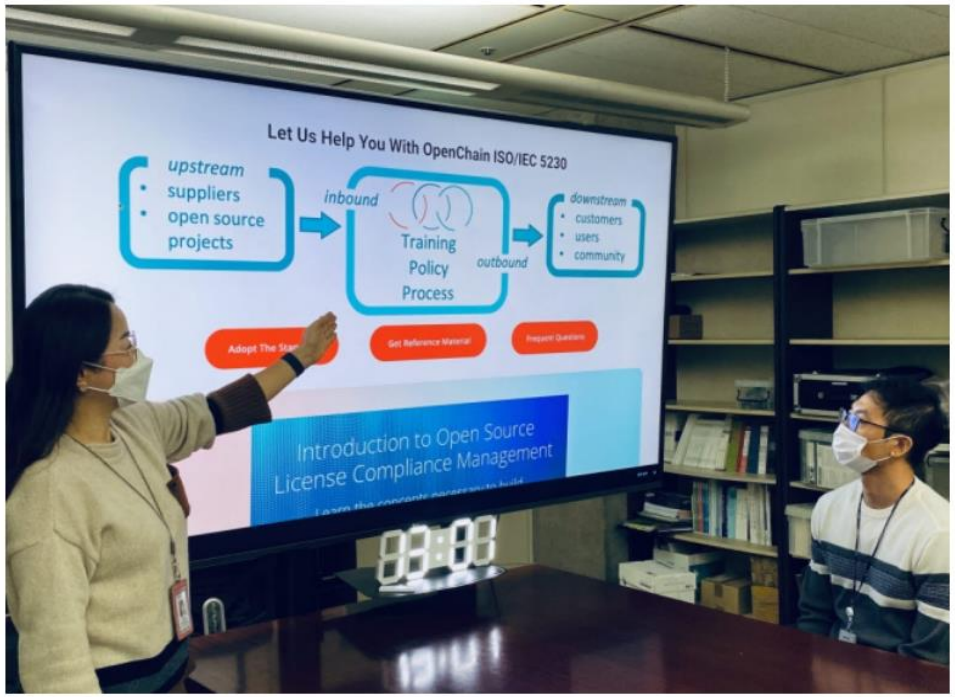
ETRI 오픈소스 SW 품질 신뢰성 제고

ETRI 오픈소스 R&D 역량 우수성 입증

전자신문

ETRI, 출연연 최초 ISO 오픈소스 국제표준 인증

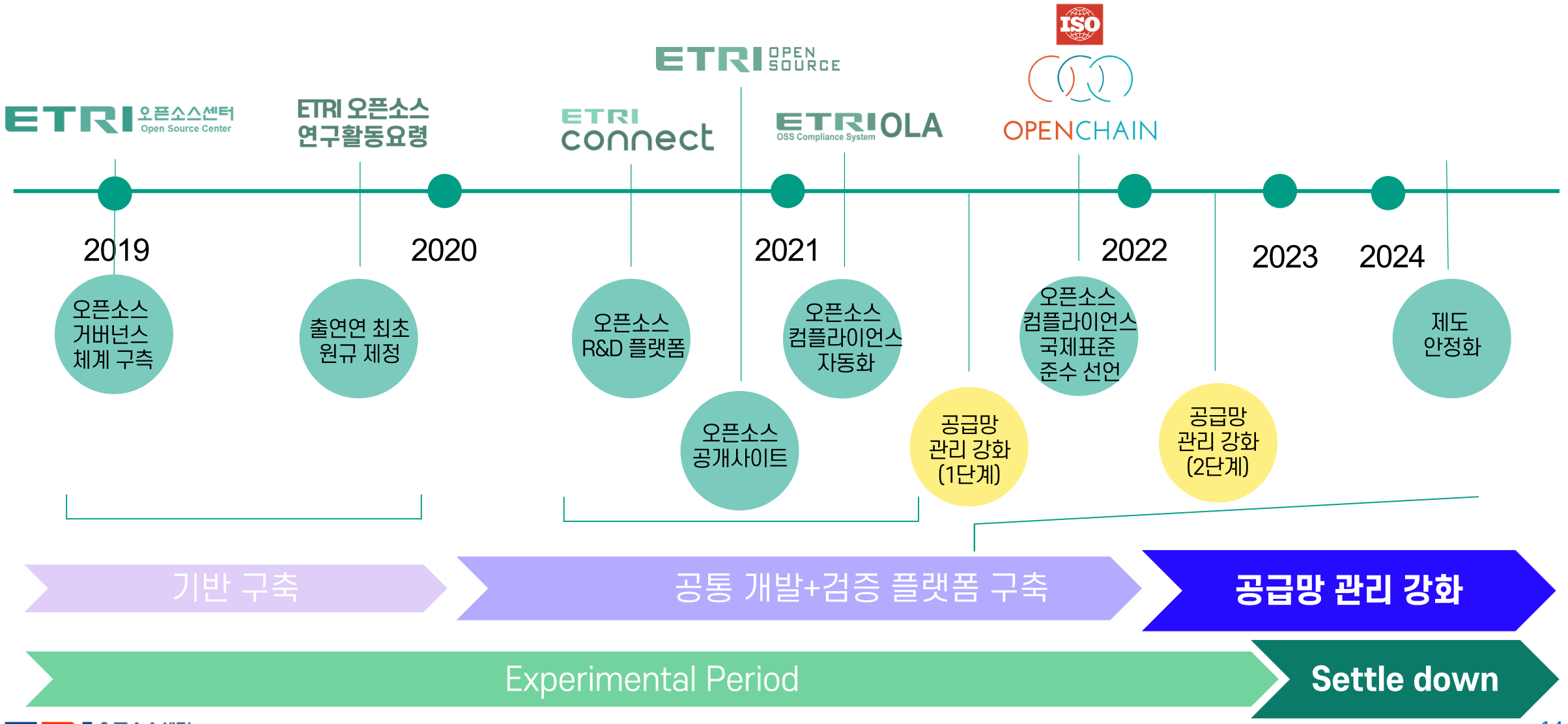
기사입력 2021-12-17 17:22



ETRI 연구진들이 오픈소스 관련 국제표준 인증과 관련, 내용을 설명하고 있다.

국내 연구진이 정부출연연구원 최초로 국제표준화기구에서 오픈소스 관련 인증을 획득하는 쾌거를 거두었다.

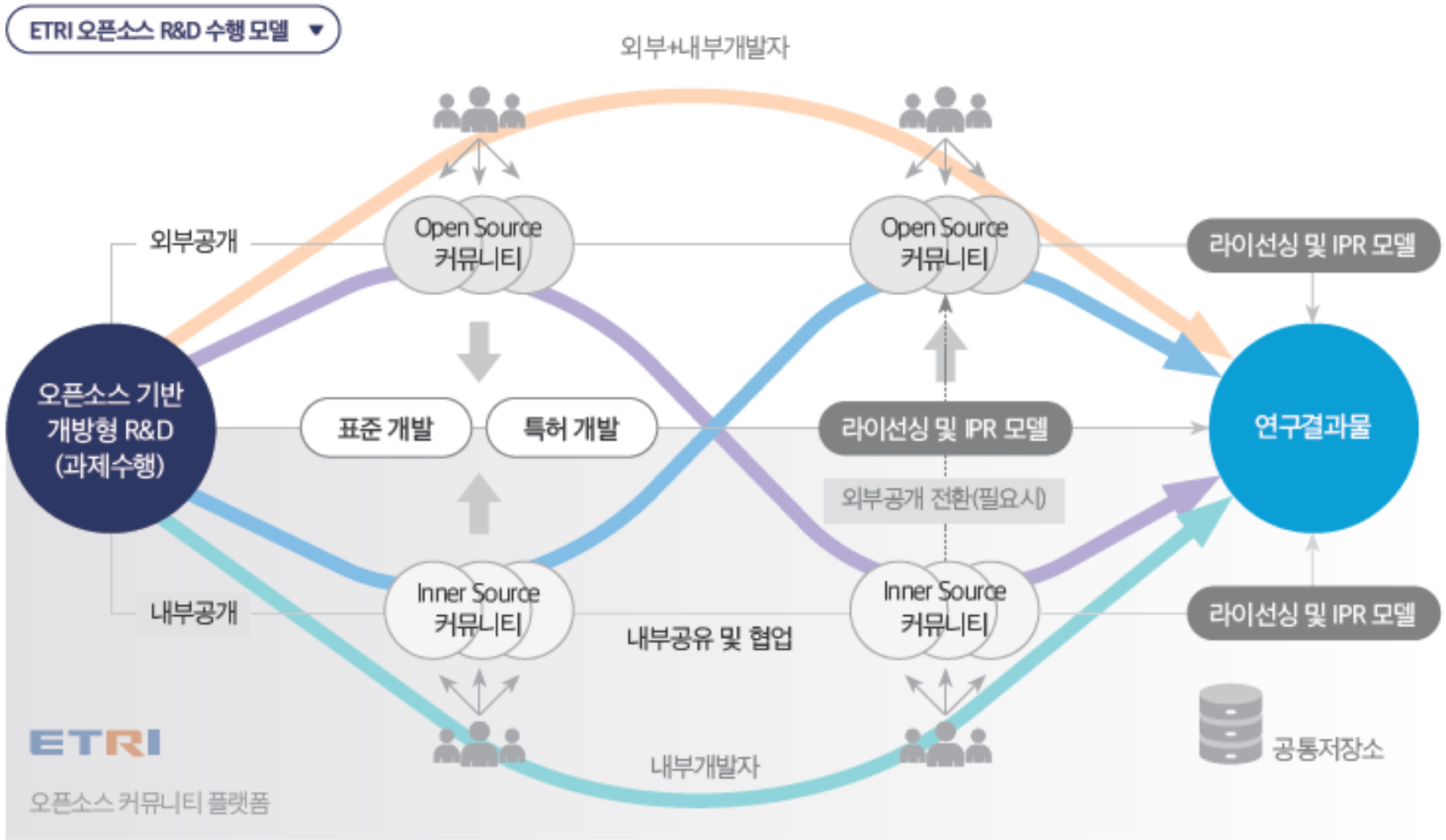
오픈소스 거버넌스 이력


ETRI 오픈소스센터 Open Source Center
ETRI 오픈소스 연구활동요령
ETRI connect
ETRI OPEN SOURCE
ETRI OLA OSS Compliance System
ISO
OPENCHAIN
2019
2020
2021
2022
2023
2024
오픈소스 거버넌스 체계 구축
출연연 최초 원규 제정
오픈소스 R&D 플랫폼
오픈소스 공개사이트
오픈소스 컴플라이언스 자동화
공급망 관리 강화 (1단계)
오픈소스 컴플라이언스 국제표준 준수 선언
공급망 관리 강화 (2단계)
제도 안정화
기반 구축
공통 개발+검증 플랫폼 구축
공급망 관리 강화
Experimental Period
Settle down

오픈소스 거버넌스 체계


ETRI 오픈소스 거버넌스 대응 체계
정부 및 유관기관
정책협력
과제수행
ISO
OPENCHAIN
ETRI 오픈소스 거버넌스
국제표준인증('21.12)
기획/행정
품질관리
지식공유
제도기획
사업 관리
기술이전
지식재산
구매조달
홍보
업무협력
전문위원제도
컴플라이언스
클리어링 하우스
EOSC
ETRI
가이드
오픈소스 위원회
연구부서
커뮤니티 활동 가이드라인
커뮤니티 플랫폼 (협업+저장소)
비즈니스 모델 제공
커뮤니티/커미터 활동지원
교육 및 컨설팅
개방형 R&D 커뮤니티
외부 오픈소스 커뮤니티
개방형 R&D 커뮤니티
개방형 오픈소스 R&D 플랫폼
기술지원
활동지원
기업 및 커뮤니티

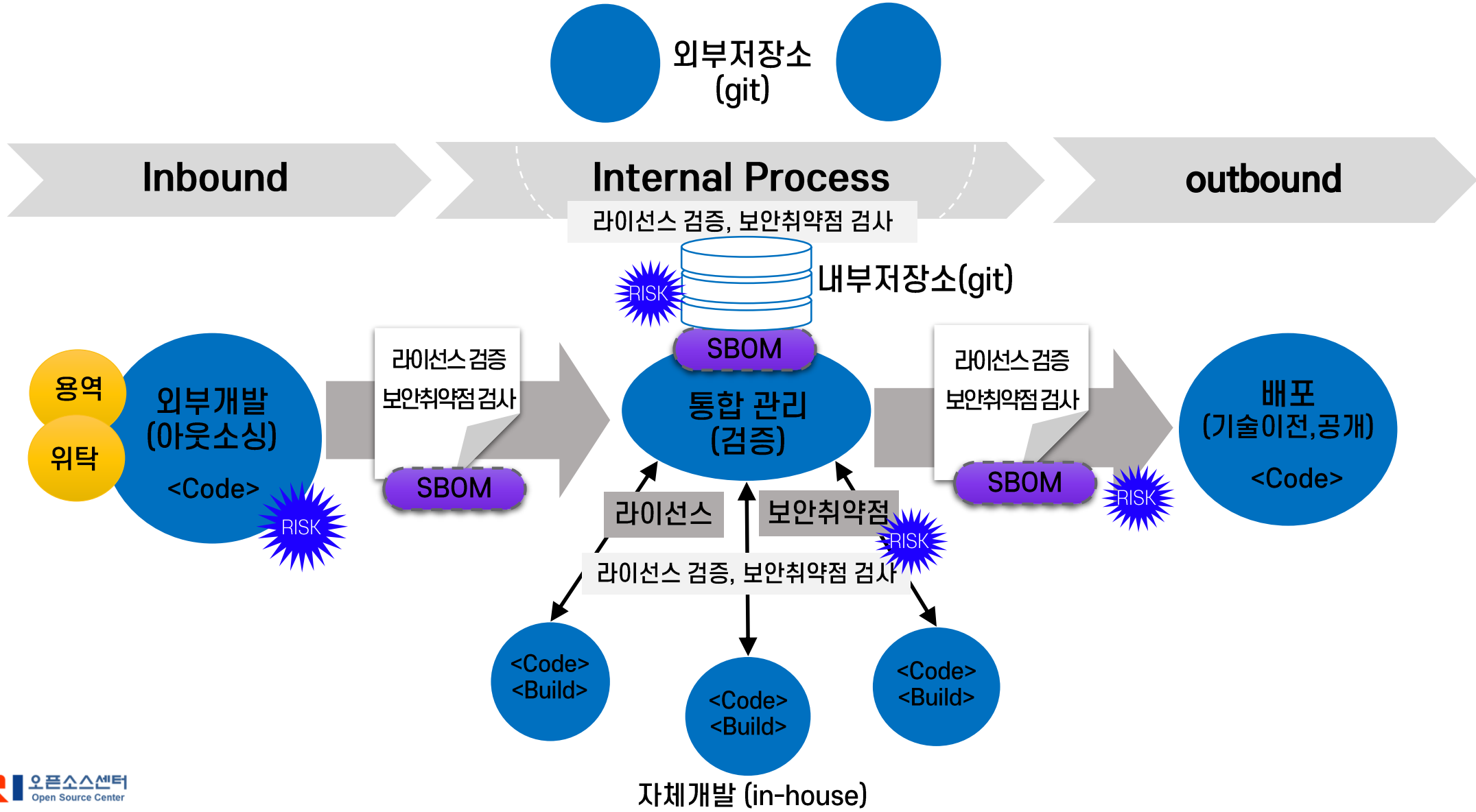
오픈소스 R&D 수행 모델


ETRI 오픈소스 R&D 수행 모델
외부+내부개발자
외부공개
Open Source 커뮤니티
Open Source 커뮤니티
라이선싱 및 IPR 모델
오픈소스 기반 개방형 R&D (과제수행)
표준 개발
특허 개발
라이선싱 및 IPR 모델
연구결과물
외부공개 전환(필요시)
내부공개
Inner Source 커뮤니티
내부공유 및 협업
Inner Source 커뮤니티
라이선싱 및 IPR 모델
공통저장소
내부개발자
ETRI
오픈소스 커뮤니티 플랫폼

SBOM 기반 오픈소스 컴플라이언스 구축 개념

"오픈소스 컴플라이언스 및 공급망 관리 효율성 개선"

SW 공급망 관리 체계


외부저장소
(git)
Inbound
Internal Process
outbound
라이선스 검증, 보안취약점 검사
내부저장소(git)
RISK
SBOM
용역
위탁
외부개발
(아웃소싱)
<Code>
RISK
라이선스 검증
보안취약점 검사
SBOM
통합 관리
(검증)
라이선스 검증
보안취약점 검사
SBOM
RISK
배포
(기술이전,공개)
<Code>
라이선스
보안취약점
RISK
라이선스 검증, 보안취약점 검사
<Code>
<Build>
<Code>
<Build>
<Code>
<Build>
자체개발 (in-house)

ETRI의 SW 외부 배포 방법

기술이전

공개

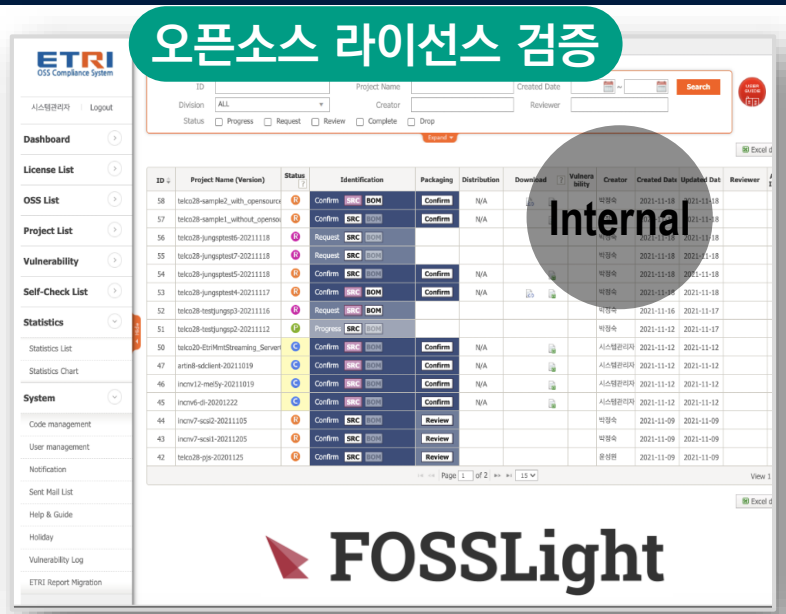
ETRI 오픈소스 R&D 플랫폼

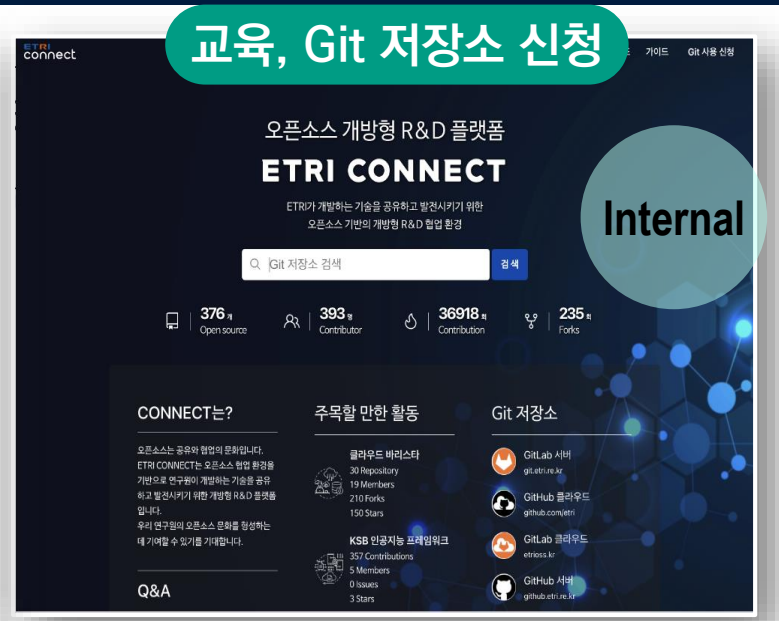
오픈소스 기반 R&D 활동지원을 위한 다양한 플랫폼 제공

ETRI OLA
OSS Compliance System
Powered by **FOSSLight**

ETRI connect

ETRI OPEN SOURCE
https://opensource.etri.re.kr





저장소 구축 및 운영 현황

- 오픈소스 연구 개발
- **공동연구 협업 개발 (용역, 위탁 포함)**
- **오픈소스 커뮤니티 활동**

GitLab

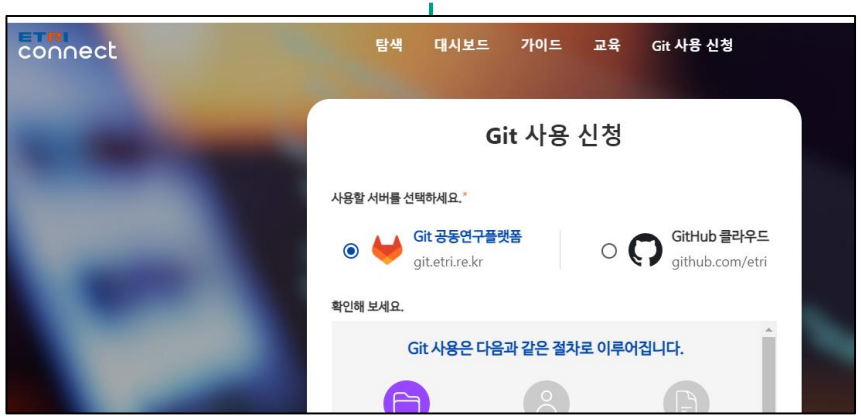
SW 공동연구 플랫폼

GitHub

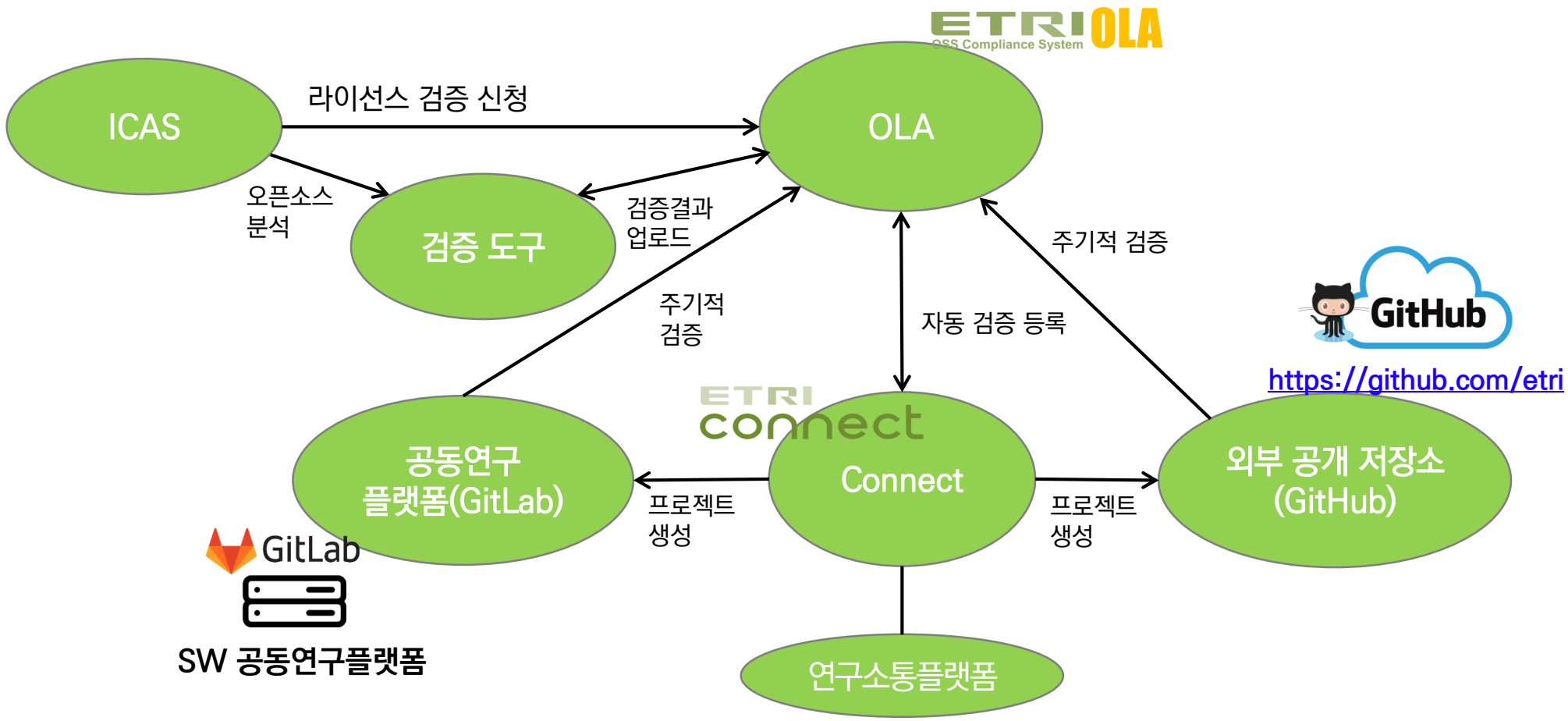
GitHub 클라우드

https://github.com/etri

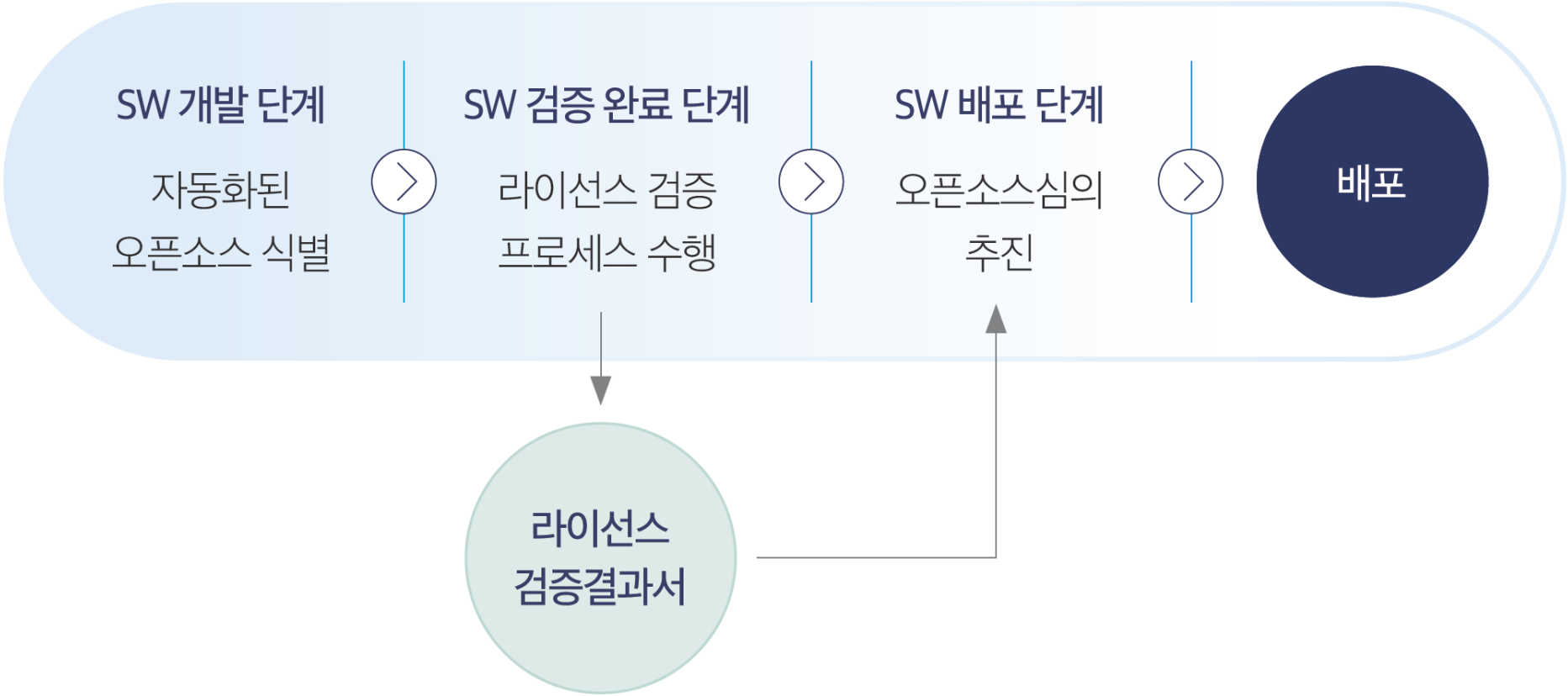
- ETRI **오픈소스 공개**
- 기술이전
- **커뮤니티 지원**
- 공모전 및 경진대회



시스템 운영 형상


ETRI OLA
OSS Compliance System
ICAS
라이선스 검증 신청
OLA
오픈소스
분석
검증 도구
검증결과
업로드
주기적 검증
주기적
검증
자동 검증 등록
GitHub
https://github.com/etri
ETRI
connect
공동연구
플랫폼(GitLab)
Connect
외부 공개 저장소
(GitHub)
프로젝트
생성
프로젝트
생성
GitLab
SW 공동연구플랫폼
연구소통플랫폼

오픈소스 컴플라이언스 프로세스



ETRI 오픈소스 관련 제도 Since 2019

- 제도 및 정책
- 표준 프로세스

- 기술이전
- 공개계획

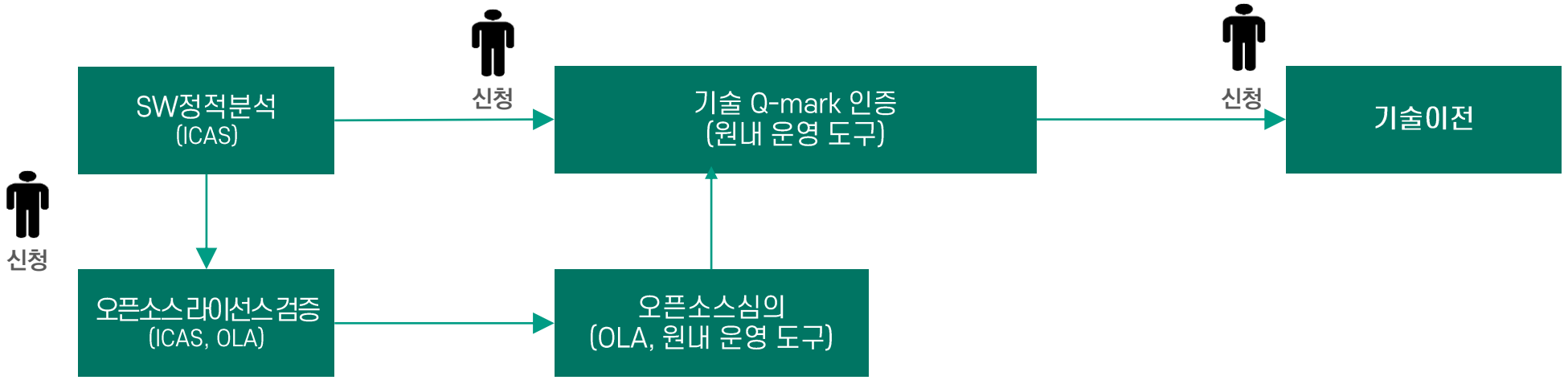
- 기술이전
- 공개계획

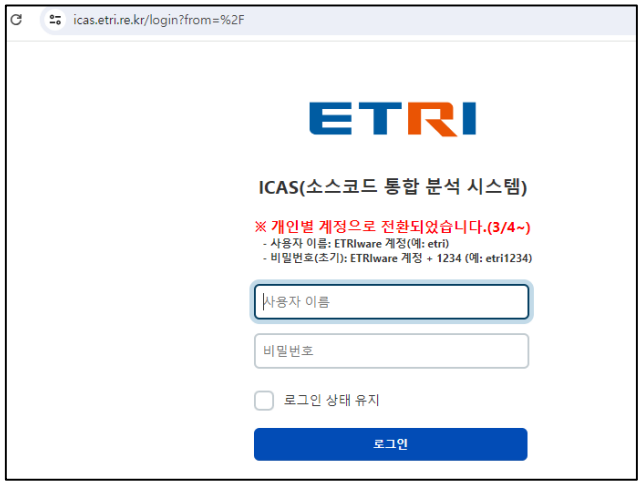
- 용역/위탁

오픈소스 원규(요령)

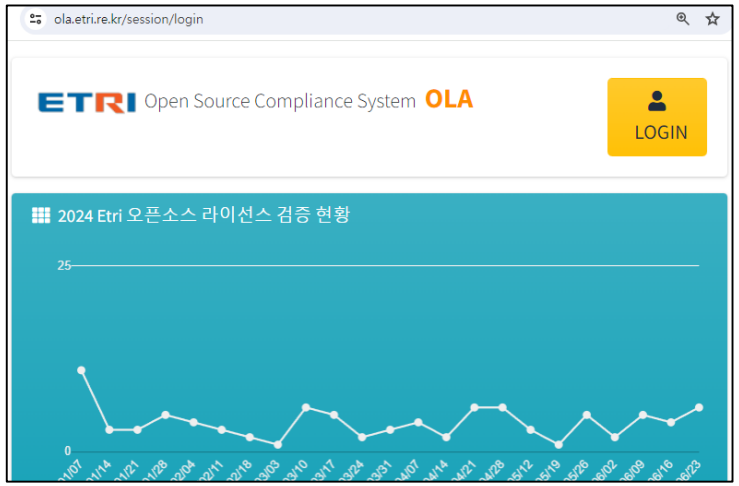
오픈소스연구활동요령 제정 (2020.1.1.부 시행) *출연연 최초

SW 외부 배포 프로세스 예: 기술이전



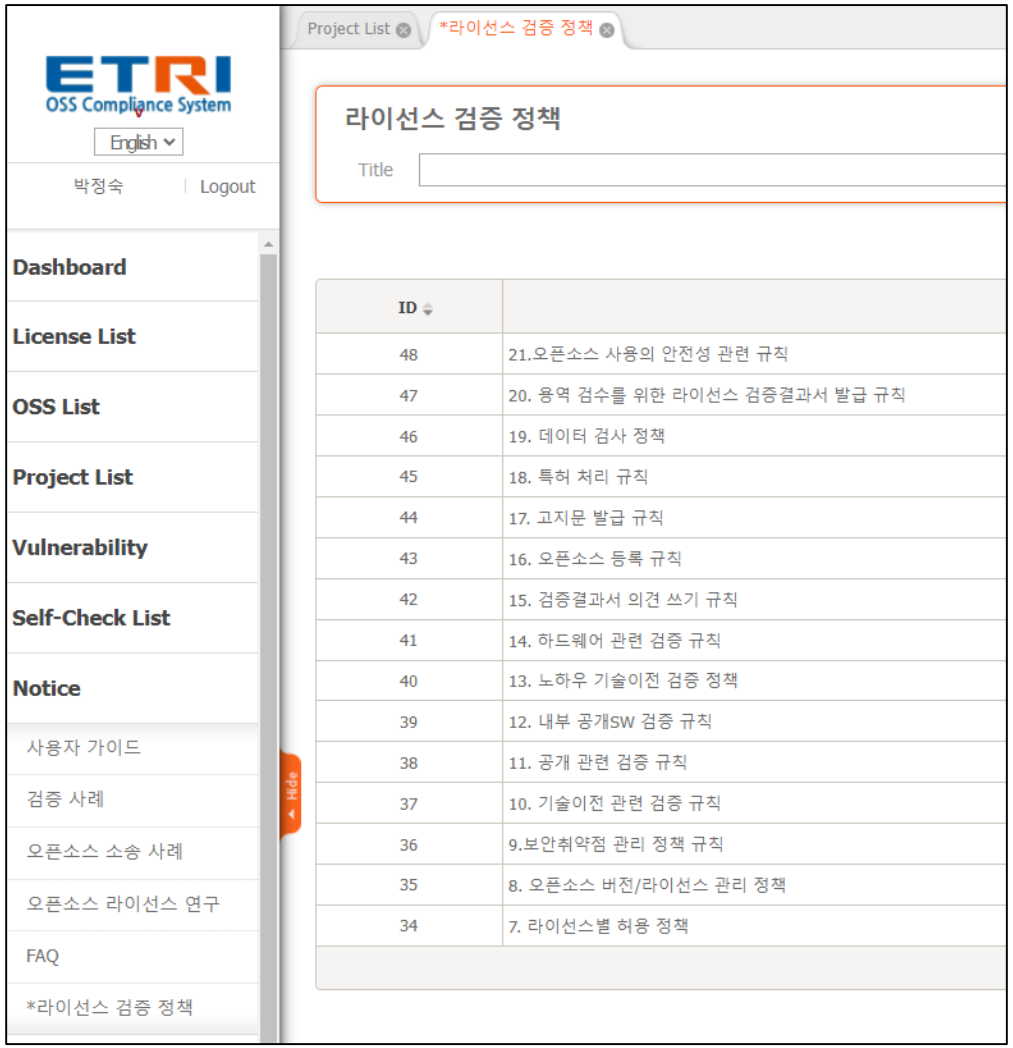


ICAS(integrated Code Analysis System)



OLA(OSS License Automation)

오픈소스 라이선스 검증 정책



SW 공급망 관리 방법 개선

- 용역의 오픈소스 관리 자율 시행
  - ➢ 용역의 오픈소스 관리 지원 페이지 제공

오픈소스 사용 관리

- 오픈소스 사용 고지문 작성 가이드라인
- 외주(용역, 위탁)는 필요한 경우 라이선스 검증 수행 권고. 대신 오픈소스 사용내역서는 필수 제출

3 고지문 작성 가이드(안)

❍ 고지문 작성 원칙

- 배포하는 소스코드 홈 디렉토리에 "NOTICE" 파일에 오픈소스 사용 내용 고지
- 오픈소스 코드 수정 시 NOTICE 파일에는 수정 내용 간략히 기술
  ▷ 수정된 해당 코드에 주석문으로 필요한 모든 사항 설명함

❍ 고지문 작성 방법 ([부록.1] 예시 참고)

단계1	NOTICE 파일 생성(위치: 코드가 위치한 루트 디렉토리)
단계2	NOTICE 파일에 사용한 오픈소스 정보 리스트 기술 • 오픈소스 정보: 오픈소스명, 버전, 웹페이지 주소, Copyright 문구, 라이선스, 수정 내용
단계3	관련 라이선스 원문 리스트 기술
단계4	파일을 저장하고 닫기
<고지문 작성 시 주의사항>	

〈오픈소스 사용 고지문 작성 가이드라인〉

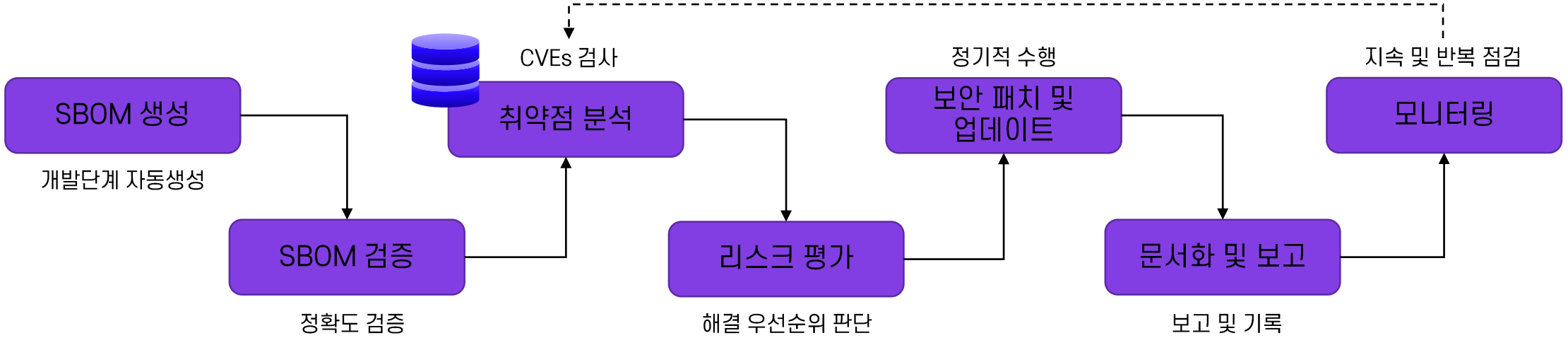
- 고지문 파일 포맷

사용 오픈소스 리스트	오픈소스명	필수
	버전 정보 ※ *버전 없는 경우는 "-"로 표기*	필수
	웹사이트 주소	필수
	Copyright 문구 (Copyright 문구 없는 경우는 저작권자 표기) ※ *예: "Copyright [년도]. ETRI. All rights reserved"* ※ *해당 정보가 있는 링크 주소를 기술해도 무방*	옵션
	라이선스: SPDX 표기법 ※ *https://spdx.org/licenses 참고*	필수
	수정 내용 (수정 내용이 있는 경우만 간략히 기술, 없으면 빈칸으로 둠) ※ *예: "Plugin 기능 추가 개발"*	옵션
라이선스 원문 리스트	라이선스 원문 링크 또는 텍스트로 기술 가능	필수

〈오픈소스 사용고지문 (사용내역서) 포맷〉

Cf) SBOM 기반 적합성 시험 방법(안)

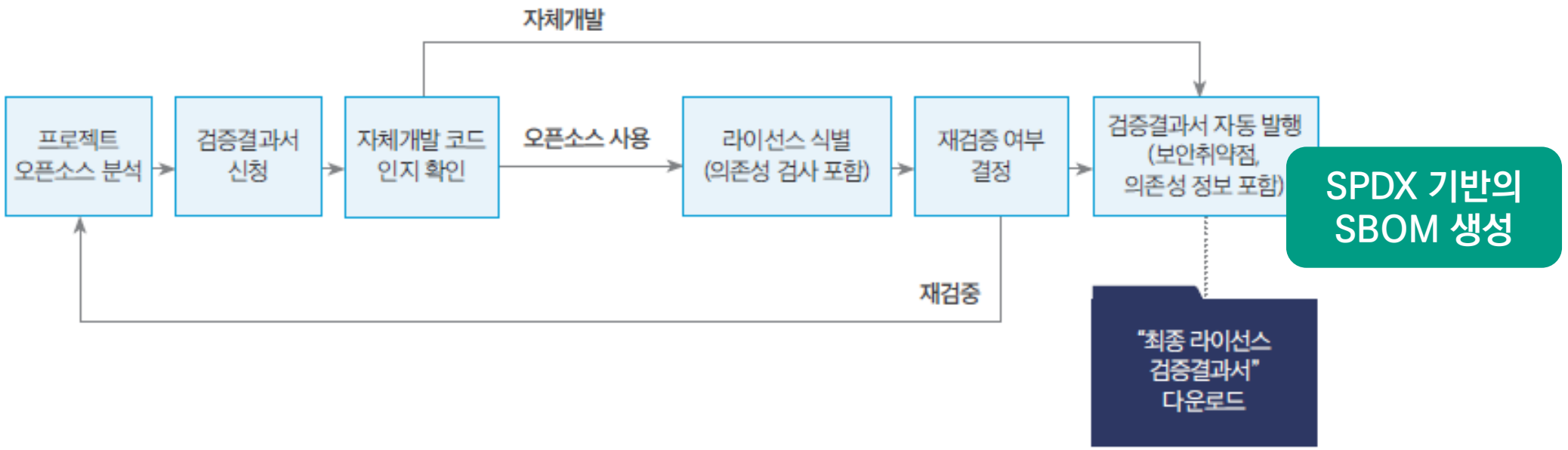
SBOM 기반 보안 적합성 시험은 SW의 구성 요소, 즉 사용된 모든 라이브러리와 의존성을 파악하여 보안 취약점을 확인하고 관리하는 프로세스



- NVD의 보안취약점 정보를 매일 크롤링하여 OLA의 보안취약점 DB 업데이트
- 새로운 보안취약점 발견 시 OLA의 해당 프로젝트에 alarm

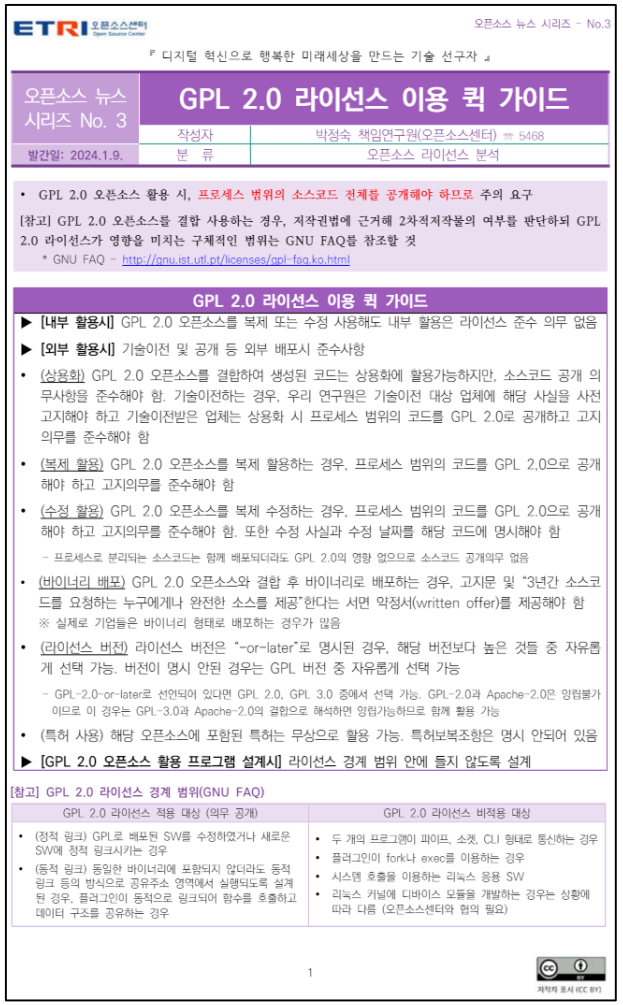
SBOM 생성 방법

- 라이선스 검증 절차를 통해 오픈소스 및 관련 정보 식별하여 SPDX 기반의 SBOM 생성



- NVD의 보안취약점 정보를 매일 크롤링하여 OLA의 보안취약점 DB 업데이트
- 새로운 보안취약점 발견 시 OLA의 해당 프로젝트에 alarm

교육



ETRI 오픈소스센터 오픈소스 뉴스 시리즈 - No.3

『 디지털 혁신으로 행복한 미래세상을 만드는 기술 선구자 』

오픈소스 뉴스 시리즈 No. 3

GPL 2.0 라이선스 이용 쿼 가이드

작성자: 박정숙 책임연구원(오픈소스센터) ☎ 5468

발간일: 2024.1.9. 분 류: 오픈소스 라이선스 분석

- GPL 2.0 오픈소스 활용 시, 프로세스 범위의 소스코드 전체를 공개해야 하므로 주의 요구

[참고] GPL 2.0 오픈소스를 결합 사용하는 경우, 저작권법에 근거해 2차적저작물의 여부를 판단하되 GPL 2.0 라이선스가 영향을 미치는 구체적인 범위는 GNU FAQ를 참조할 것

* GNU FAQ - http://gnu.ist.utl.pt/licenses/gpl-faq.ko.html

GPL 2.0 라이선스 이용 쿼 가이드

▶ **[내부 활용시]** GPL 2.0 오픈소스를 복제 또는 수정 사용해도 내부 활용은 라이선스 준수 의무 없음

▶ **[외부 활용시]** 기술이전 및 공개 등 외부 배포시 준수사항

- (상용화) GPL 2.0 오픈소스를 결합하여 생성된 코드는 상용화에 활용가능하지만, 소스코드 공개 의무사항을 준수해야 함. 기술이전하는 경우, 우리 연구원은 기술이전 대상 업체에 해당 사실을 사전 고지해야 하고 기술이전받은 업체는 상용화 시 프로세스 범위의 코드를 GPL 2.0로 공개하고 고지의무를 준수해야 함
- (복제 활용) GPL 2.0 오픈소스를 복제 활용하는 경우, 프로세스 범위의 코드를 GPL 2.0으로 공개해야 하고 고지의무를 준수해야 함
- (수정 활용) GPL 2.0 오픈소스를 복제 수정하는 경우, 프로세스 범위의 코드를 GPL 2.0으로 공개해야 하고 고지의무를 준수해야 함. 또한 수정 사실과 수정 날짜를 해당 코드에 명시해야 함
  - 프로세스로 분리되는 소스코드는 함께 배포되더라도 GPL 2.0의 영향 없으므로 소스코드 공개의무 없음
- (바이너리 배포) GPL 2.0 오픈소스와 결합 후 바이너리로 배포하는 경우, 고지문 및 "3년간 소스코드를 요청하는 누구에게나 완전한 소스를 제공"한다는 서면 약정서(written offer)를 제공해야 함
  ※ 실제로 기업들은 바이너리 형태로 배포하는 경우가 많음
- (라이선스 버전) 라이선스 버전은 "-or-later"로 명시된 경우, 해당 버전보다 높은 것들 중 자유롭게 선택 가능. 버전이 명시 안된 경우는 GPL 버전 중 자유롭게 선택 가능
  - GPL-2.0-or-later로 선언되어 있다면 GPL 2.0, GPL 3.0 중에서 선택 가능. GPL-2.0과 Apache-2.0은 양립불가이므로 이 경우는 GPL-3.0과 Apache-2.0의 결합으로 해석하면 양립가능하므로 함께 활용 가능
- (특허 사용) 해당 오픈소스에 포함된 특허는 무상으로 활용 가능. 특허보복조항은 명시 안되어 있음

▶ **[GPL 2.0 오픈소스 활용 프로그램 설계시]** 라이선스 경계 범위 안에 들지 않도록 설계

[참고] GPL 2.0 라이선스 경계 범위(GNU FAQ)

GPL 2.0 라이선스 적용 대상 (의무 공개)	GPL 2.0 라이선스 비적용 대상
• (정적 링크) GPL로 배포된 SW를 수정하였거나 새로운 SW에 정적 링크시키는 경우 • (동적 링크) 동일한 바이너리에 포함되지 않더라도 동적 링크 등의 방식으로 공유주소 영역에서 실행되도록 설계된 경우, 플러그인이 동적으로 링크되어 함수를 호출하고 데이터 구조를 공유하는 경우	• 두 개의 프로그램이 파이프, 소켓, CLI 형태로 통신하는 경우 • 플러그인이 fork나 exec를 이용하는 경우 • 시스템 호출을 이용하는 리눅스 응용 SW • 리눅스 커널에 디바이스 모듈을 개발하는 경우는 상황에 따라 다름 (오픈소스센터와 협의 필요)

1

저작자 표시 (CC BY)

03

향후 계획

향후 계획

- 도구의 자동화
  - 확장성
  - 속도
  - 정확성
- Shift-Left
- 교육 및 컨설팅을 통한 인식 제고

감사합니다.

ETRI 오픈소스센터
박정숙 센터장

jungsp@etri.re.kr, 010-8849-6513