블록체인 기반 SBOM의 무결성 검증 시스템

*SBOM(Software Bill of Materials)

임지현 | 김호석 | 문준호

OVERVIEW

1. 시스템 소개

- SBOM이란?
- 기존 시스템 현황
- 필요성 및 차별성

2. 시스템 설계

- 기존 시스템 구조
- 개선된 시스템 구조
- 시스템 흐름도
- 시스템 주요 기능
- 개발 환경

3. 향후 수행 계획 및 기대 효과

- 역할 분담
- 추진 일정
- 기대 효과

1. SBOM 이란?

SBOM(Software Bill of Material)은 직역하면 소프트웨어 자재 명세서
최종 고객이 사용하는 소프트웨어 혹은 서비스를 완성하기 위해 활용되는 모든 소프트웨어 정보를 담고 있는 명세서라고 할 수 있다.

영양정보

총 내용량 1,000 g
100g당 240 kcal

			1일 영양성분 기준치에 대한 비율
나트륨	160	mg	8 %
탄수화물	59	g	18 %
당류	57	g	57 %
지방	0.2	g	0 %
트랜스지방	0	g	
포화지방	0	g	0 %
콜레스테롤	0	mg	0 %
단백질	0	g	0 %

1일 영양성분 기준치에 대한 비율(%)은 2,000 kcal 기준이므로 개인의 필요 열량에 따라 다를 수 있습니다.

제품명	카페베네 청포도청
식품유형	음료베이스
내용량	1,000g (2,400 kcal)
제조원	(주)다정/경기도 포천시 영중면 영일로 97번길 28
유통전문판매원	(주)카페베네/서울 성동구 상원1길 25, 901 빌딩 8층
포장재질	유리 (뚜껑 : 주석도금강판)
유통기한	별도 표기일까지
품목보고번호	19990372301-592
원재료명 및 함량	포도당함유[포도**농축액**(**중국산** 50%, 설탕(35%, 설탕, 정제수, 기타과당), 청포도농축액(**칠레산** 고형분함량30%)2%, 구연산, 청포도향, 청포도향베이스, 포도향베이스, 프로필렌글리콜, 조정, 혼합제제(카라기난, 로커스트콩검, 염화칼륨, 포도당, 젖산칼슘, 제이인산칼륨, 구연산삼나트륨), CMC, 구연산삼나트륨, 정제소금(**국산**), 그린칼라(홍화황색소, 치자청색소), 아스파탐(감미료)

[주의사항] -원료(과일) 특성상 색상 및 물성이 상이할 수 있으나 제품에는 하자가 없으니 안심하고 드십시오. -과일씨가 있을 수 있으나 이물질이 아니오니 안심하고 드십시오. -흔들어 드세요. -과냉각되나 하우

유리
뚜껑:철

출처: scribesecurity.com

1. SBOM 이란?

SBOM 표준 포맷

표준 포맷	설명
SPDX (Software Package Data Exchange)	• '11년 리눅스 재단에서 개발해 '21년 국제표준(ISO/IEC 5962:2021)으로 등록되었다. • 오픈소스 라이선스 관리와 SBOM 포맷 활용에 용이하며, SW 패키지와 관련된 컴포넌트, 라이선스, 저작권 및 보안 정보를 전달할 수 있다. • xls, rdf, json, yml 언어로 작성되며, SPDX는 SBOM 자동 생성 도구를 제공하며, dotnet(.net), Maven(Java), PIP(Phython) 등의 패키지 매니저를 지원하여 SW가 어떤 하위 패키지를 포함하고 있는지 정보를 추출하고 이를 SBOM으로 만든다. • SPDX 문서는 문서 생성 정보, 패키지 정보, 파일 정보, 스니핏 정보, 라이선스 정보, 컴포넌트 간의 관계 정보(종속성 정보) 및 주석 등의 필드와 데이터들로 구성된다.
SWID (Software Identity)	• NIST가 '09년에 공개하여 '15년도에 국제표준(ISO/IEC19770-2:2015)으로 등록되었다. • SW제품의 특정 릴리즈에 대한 정보를 포함하고 있으며, SW 정보에 대한 태그를 생성하여 장치에 설치된 상용 및 오픈소스 SW 인벤토리를 지원한다. • SWID 태그는 소프트웨어 생명주기와 연계되어 SW 컴포넌트에 대한 식별 정보, SW 산출물에 대한 파일 및 암호화 해시 목록, SBOM 작성자 및 SW 컴포넌트에 대한 출처 정보를 제공한다.
CycloneDX	• OWASP 단체가 사이버 위험 감소를 위해 고급 공급망 기능을 지원하는 풀스택 BOM 산업 표준을 지향하며, '17년도에 초기 프로토타입 공개를 시작으로 현재 1.4버전까지 공개하였다. 처음부터 SBOM 포맷으로 설계된 점이 특징이며 SaaSBOM을 포함한 다양한 사양을 지원한다. • JSON, XML 언어로 작성되며 빌드 시스템에 구현하여 유연하고 쉽게 채택하여 활용할 수 있다는 장점이 있으며 메타데이터, 컴포넌트, 서비스, 종속성, 구성, 취약점, 확장으로 구성되어 있다.

1. SBOM 이란?

SBOM 구성 요소 및 정보

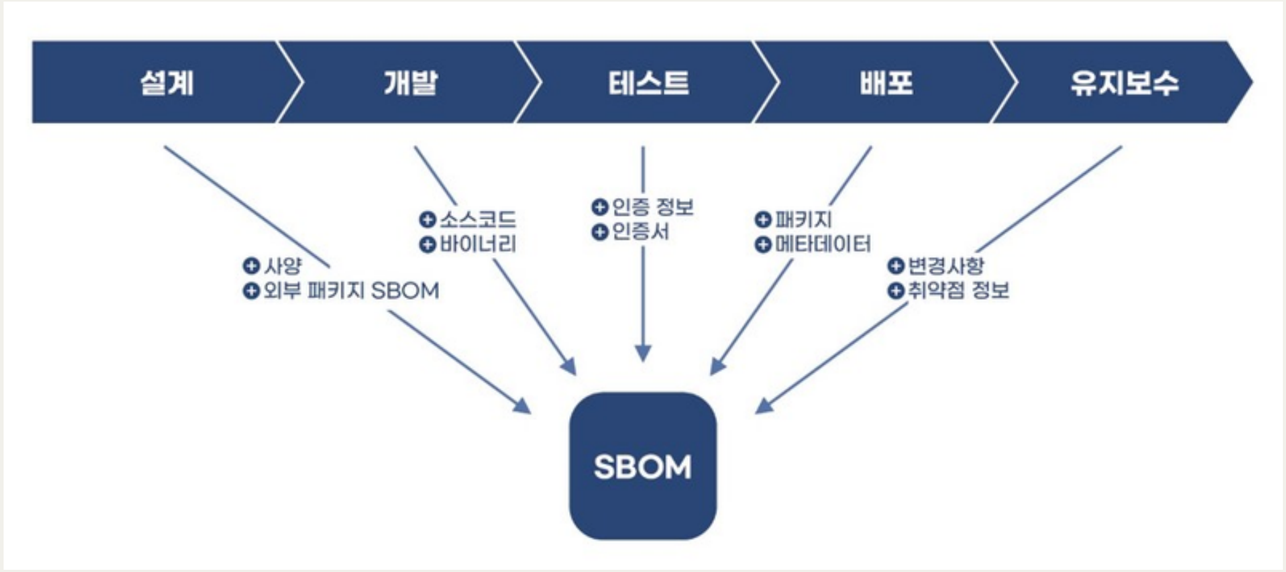
SPDX v2.3 Document shall contain:

SPDX Document Creation Information	**문서 생성 정보:** SPDX 문서 버전, 데이터 라이선스, SPDX 고육식별 번호, 문서 이름 등

SPDX v2.3 Document may contain:

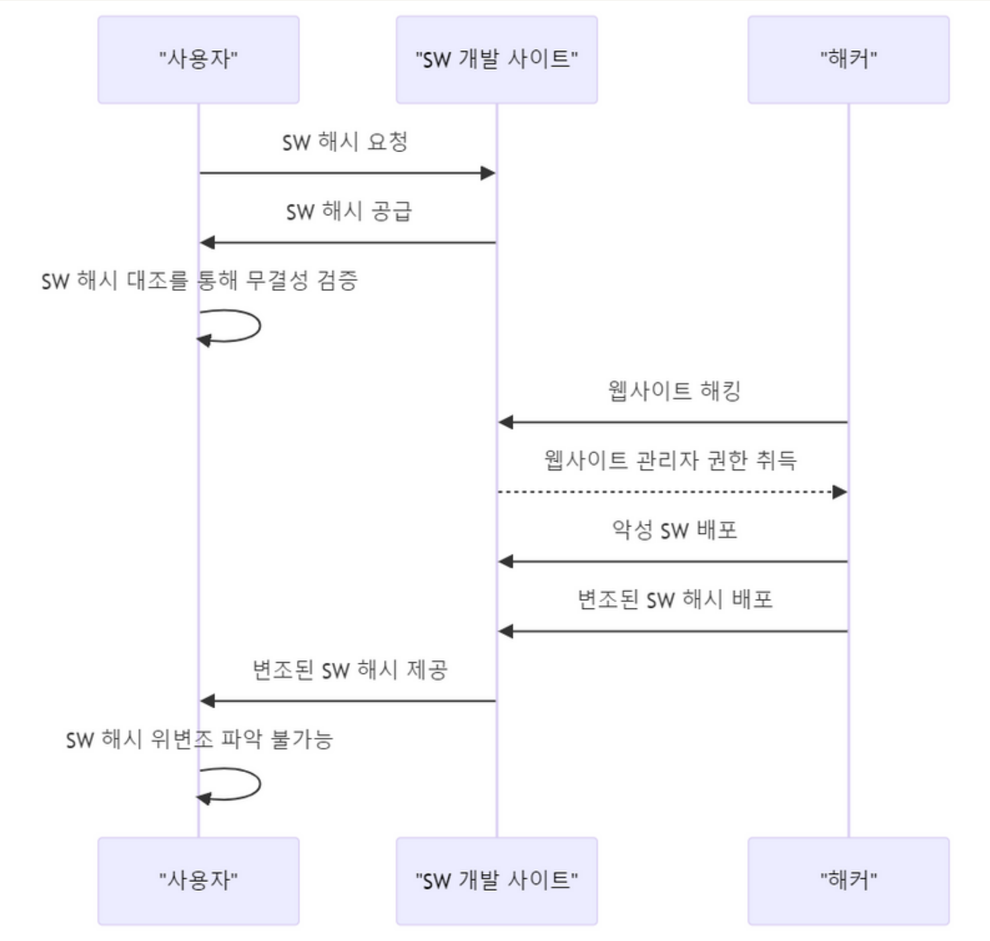
Package Information	**패키지 정보 :** 패키지 이름, 패키지 SPDX 고유번호, 패키지 정보, 패키지 파일 이름, 패키지 공급자 등
File Information	**파일 정보 :** 패키지에 포함된 각 파일의 라이선스 및 저작권 정보
Snippet Information	**스니펫 정보:** 웹이나 다른 SW 제품에서 복한 저작권 및 라이선스 조건이 첨부된 코드의 정보
Other Licensing Information Detected	**감지된 기타 라이선스 정보:** 패키지에 포함된 라이선스 중 표준에 정의되지 않은 라이선스 정보
Relationships between SPDX Elements Information	**SPDX 요소 정보 간의 관계 :** SPDX 구성요소 사이의 관계성을 나타내는 항목
Annotations Information	**주석 정보 :** 파일, 패키지 또는 전체 문서에 대한 설명을 기술
Review Information	**검토 정보 :** SPDX 2.0부터 사용하지 않음

[그림 3] SPDX 문서 구조 (출처 : 리눅스 재단)



소프트웨어 개발 주기에 따른 SBOM 정보 (출처 : 한국인터넷진흥원)

1.기존 시스템 현황



스패로우 회사의 SCA 솔루션 SBOM 무결성 검증 방식

현재 SBOM 무결성 검증 방식(컴포넌트 해시)

-> 공격자의 서버 해킹으로 인해 SW개발사에서 제공하는 SBOM의 정보 가 위·변조되어 컴포넌트 해시 또한 위·변조 될 수 있는 문제가 발생할 수 있다.

1. SBOM 이란?

20년 12월 공격 사실이 알려진 솔라윈즈 사건은 SW 기업 내부망에 침투한 후 악성코드를 제품 업데이트에 심어 유포하는 방식으로 미국 주요 정부기관과 기업들이 피해를 입은 사건

Log4j 취약점은 2021년 12월 처음 발견됐으며, 해당 취약점을 악용해 공격자가 특정 메시지를 입력하면 공격자는 원격지에서 컴퓨터 서비스 권한을 탈취할 수 있다. Log4j 취약점은 많은 소프트웨어와 플랫폼에서 사용하는 도구이기에 컴퓨터 사상 최악의 취약점으로 평가되고 있다.

2. 필요성 및 차별성

근거 1. 현재 과기부 SBOM 자동생성 및 무결성 검증 기술 개발중

- 과기부 'SW공급망 보안을 위한 SBOM 자동생성 및 무결성 검증기술 개발(2022-2025)' 연구과제 참여

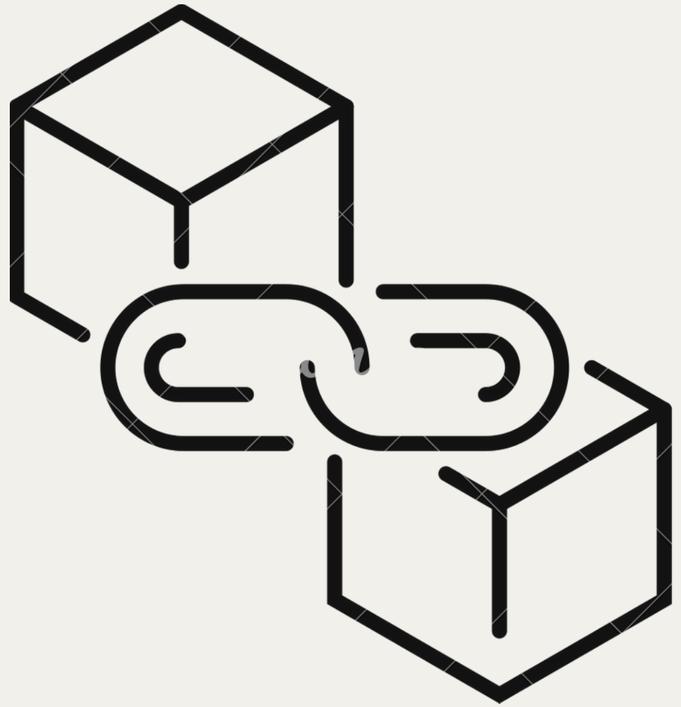
근거 2. SBOM 작성을 하지 않으면 SW 수출이 어려워짐

美 "한국 SW에 SBOM 있나요?"...국내 제도화 언제쯤?

SBOM의 중요성은 커져가고있는데,
국내는 아직까지 업계 의견수렴 단계인데다가 실증사업조차도 기초적인 수준에 머무르고 있음

2. 필요성 및 차별성

SW 개발사에서 제공하는 SBOM이 SW 사용자에게 제공되는 SBOM과 동일한 문서인지 알 수 없기 때문에 SBOM에 대한 무결성을 검증하기에 부족함이 있다.

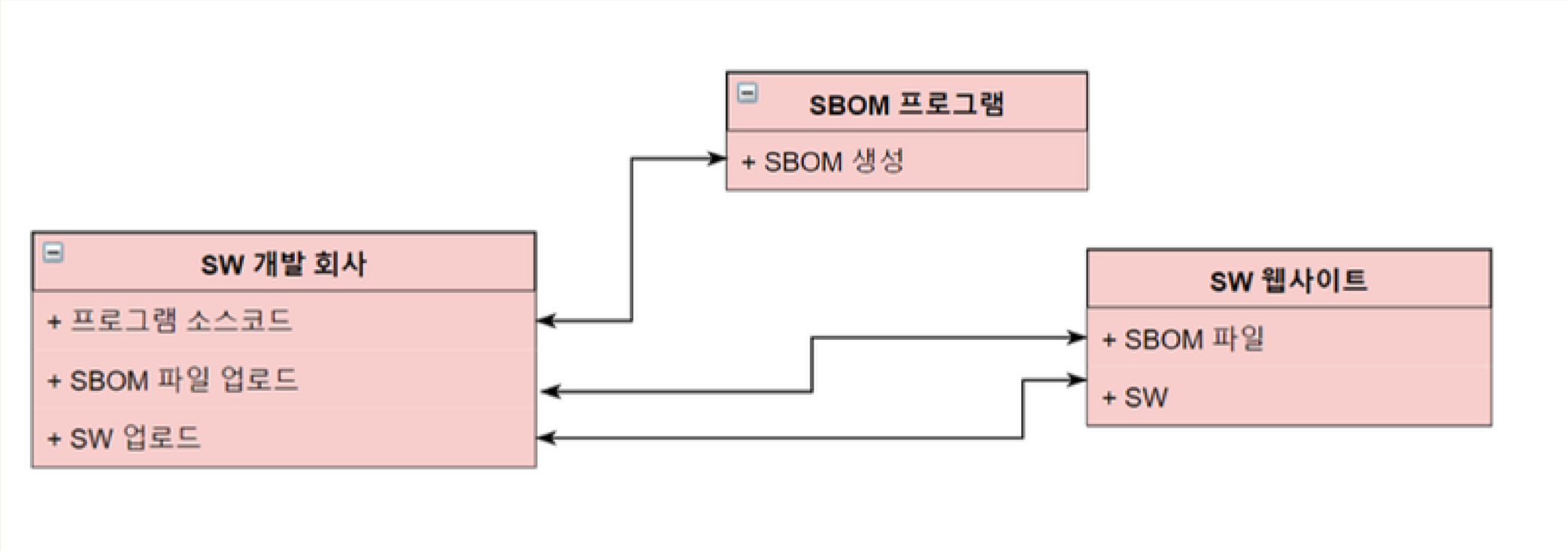


SBOM 무결성 검증기술

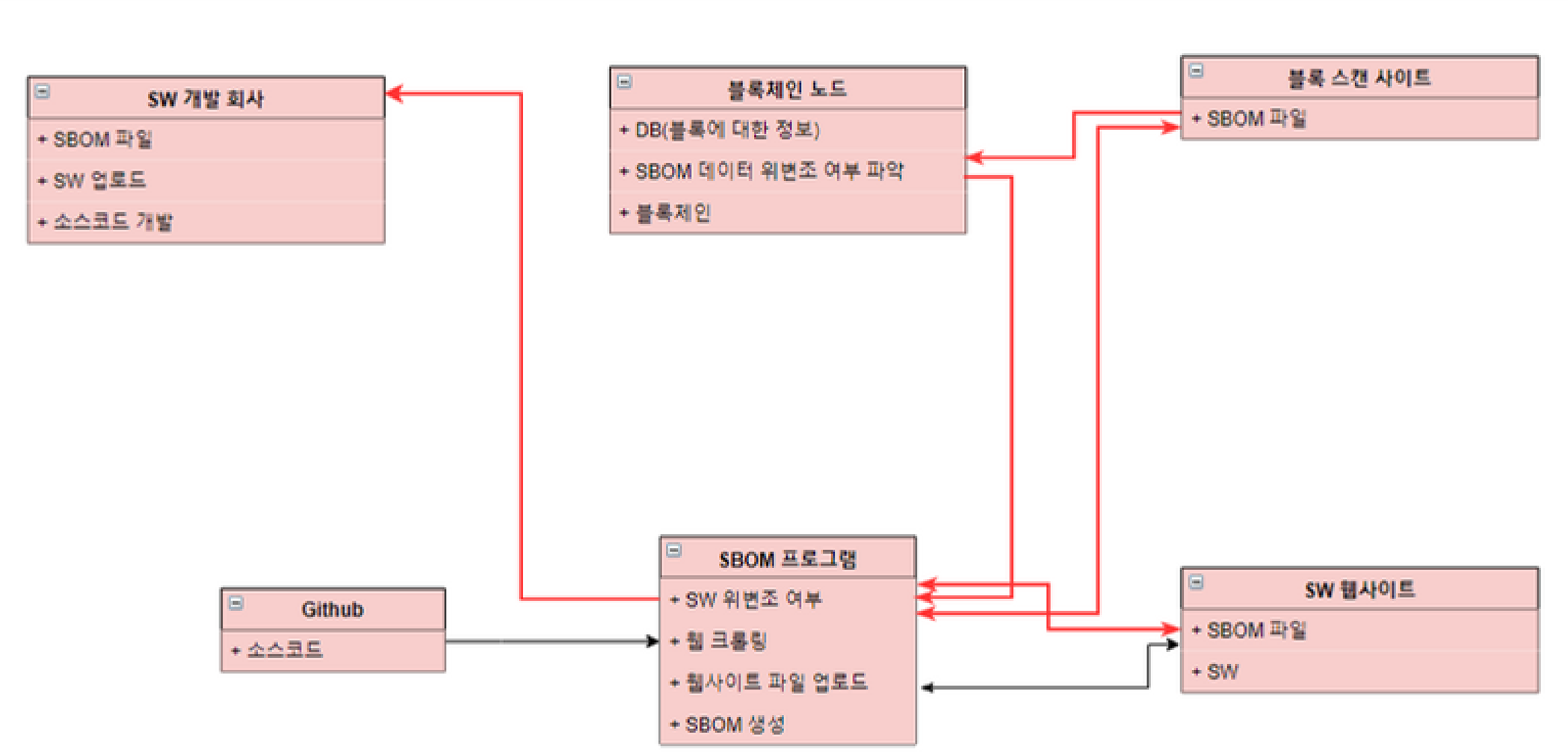
“블록체인”

차별성 : 블록체인을 통한 SBOM 무결성 검증

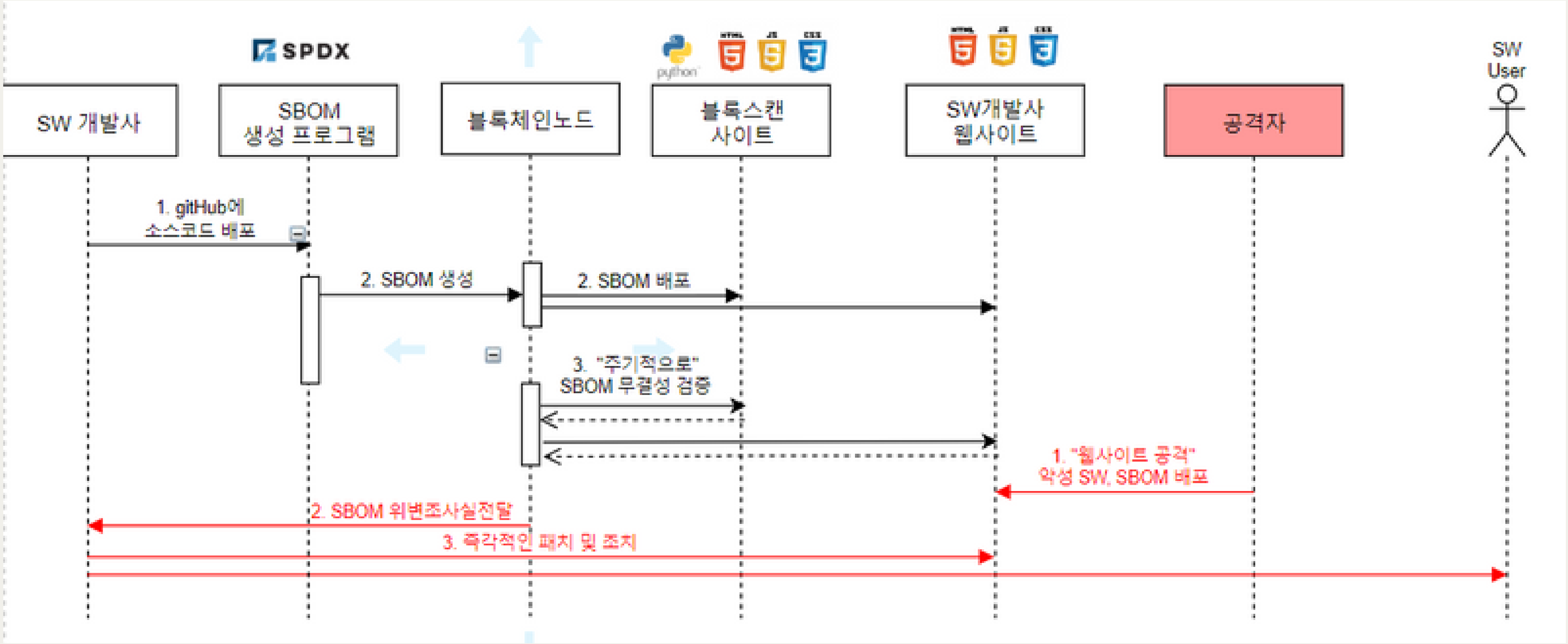
3. 기존 시스템 구조


SBOM 프로그램
+ SBOM 생성
SW 개발 회사
+ 프로그램 소스코드
+ SBOM 파일 업로드
+ SW 업로드
SW 웹사이트
+ SBOM 파일
+ SW

3. 제안하는 시스템 구조


SW 개발 회사
+ SBOM 파일
+ SW 업로드
+ 소스코드 개발
블록체인 노드
+ DB(블록에 대한 정보)
+ SBOM 데이터 위변조 여부 파악
+ 블록체인
블록 스캔 사이트
+ SBOM 파일
Github
+ 소스코드
SBOM 프로그램
+ SW 위변조 여부
+ 웹 크롤링
+ 웹사이트 파일 업로드
+ SBOM 생성
SW 웹사이트
+ SBOM 파일
+ SW

3. 시스템 흐름도 – 블록체인 추가



3. 시스템 주요 기능

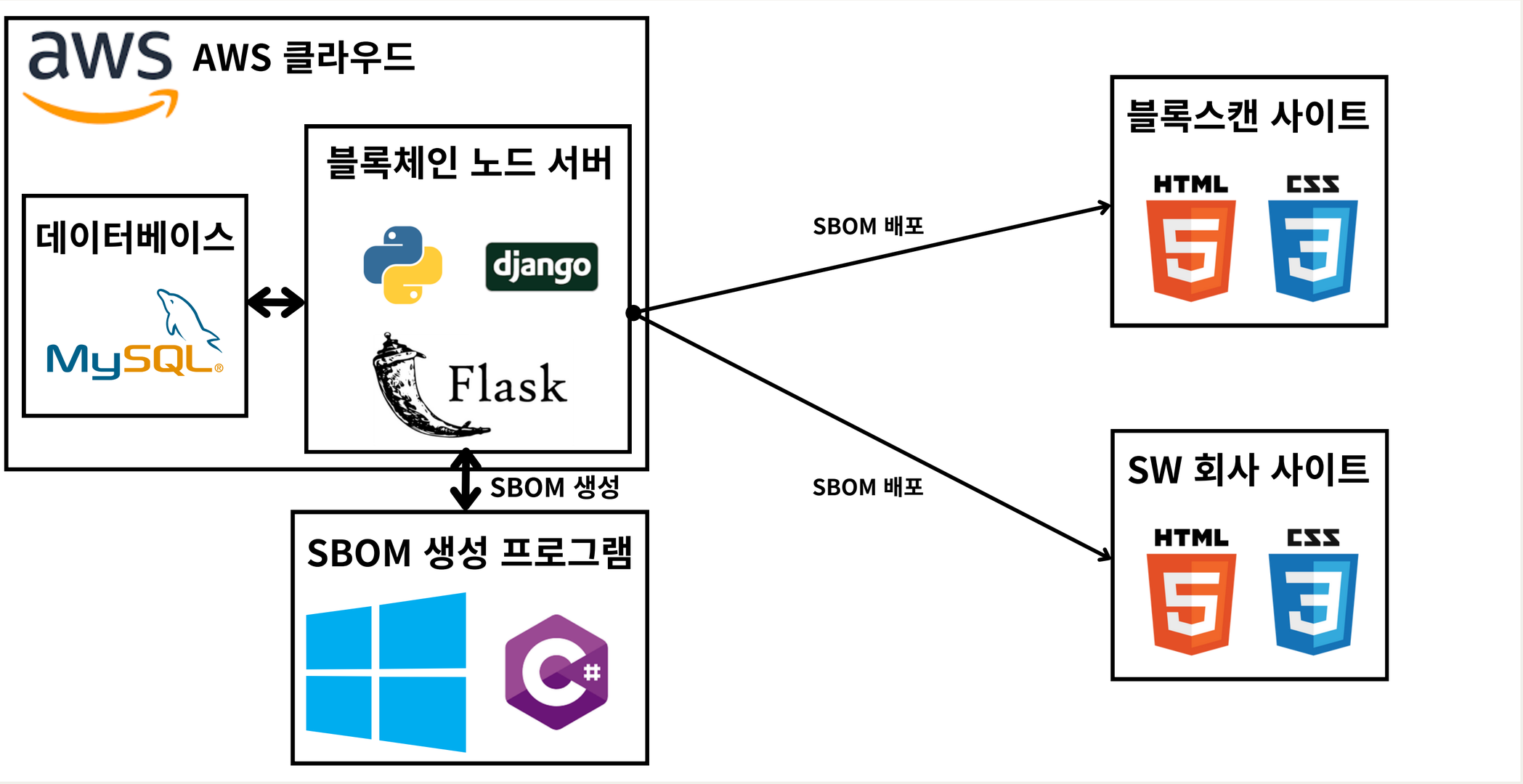
SBOM 프로그램

- SBOM 생성
- SBOM 웹사이트 배포 자동화
- 소스코드 정적 분석
- 소스코드 분석

블록체인 노드

- 이더리움기반 퍼블릭 블록체인 노드 구축
- SBOM 파일을 DB에 업데이트
- 웹 크롤링을 통한 블록체인 스캔 사이트 위·변조 여부 파악
- POS 방식의 합의 알고리즘 방식

3. 개발 환경


AWS 클라우드
데이터베이스
MySQL
블록체인 노드 서버
django
Flask
SBOM 생성
SBOM 생성 프로그램
SBOM 배포
SBOM 배포
블록스캔 사이트
HTML
CSS
SW 회사 사이트
HTML
CSS

3. 역할 분담

김호석

블록체인 노드 개발

이더리움 네트워크 구성

스마트 컨트랙트 개발

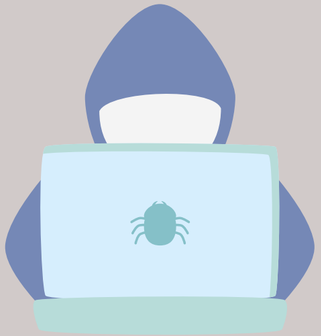
임지현

웹사이트 구축

- 블록체인 스캔사이트

SBOM 프로그램 기능

- 웹 크롤링
- Snyk 취약점 분석



문준호

SBOM 생성 툴 개발

API 서버 구축

데이터베이스 구축

3. 추진 일정

대분류	중분류	항목	9	10	11	12	1	2	3	4	5	6
계획	프로젝트 주제 선정	개인별 아이디어 조사										
		팀별 주제 선정 및 자료조사										
		중간발표										
개발	블록체인 개발	블록체인 노드 구축										
		블록체인 스캔 사이트 구축										
		SBOM 위변조 검증										
	SBOM 생성 프로그램 개발	SBOM 생성 프로그램										
		SBOM 파일 배포 자동화										
테스트	보고서 작성 및 프로젝트 마무리	프로그램 테스트										
		최종 결과 보고서 작성										
		최종 발표										

4. 기대 효과

경제적 기대효과

- 소프트웨어 개발 및 유지보수 비용 절감
- 효율적인 개발 및 유지보수 가능
- 보안 문제 신속 파악 및 해결 비용 및 시간 절감

사회적 기대효과

- 더 안전한 소프트웨어 환경 경험 가능
- SW에 대한 신뢰성 높아짐
- 정보 보호 인식 증진

산업적 기대효과

- 소프트웨어 산업 표준화 촉진
- 산업 전반의 품질 향상 및 혁신 도모
- 소프트웨어 구성 요소 투명성 보안 강화, 라이선스 준수 등을 통해 산업 건전성 높이기

THANK YOU

감사합니다