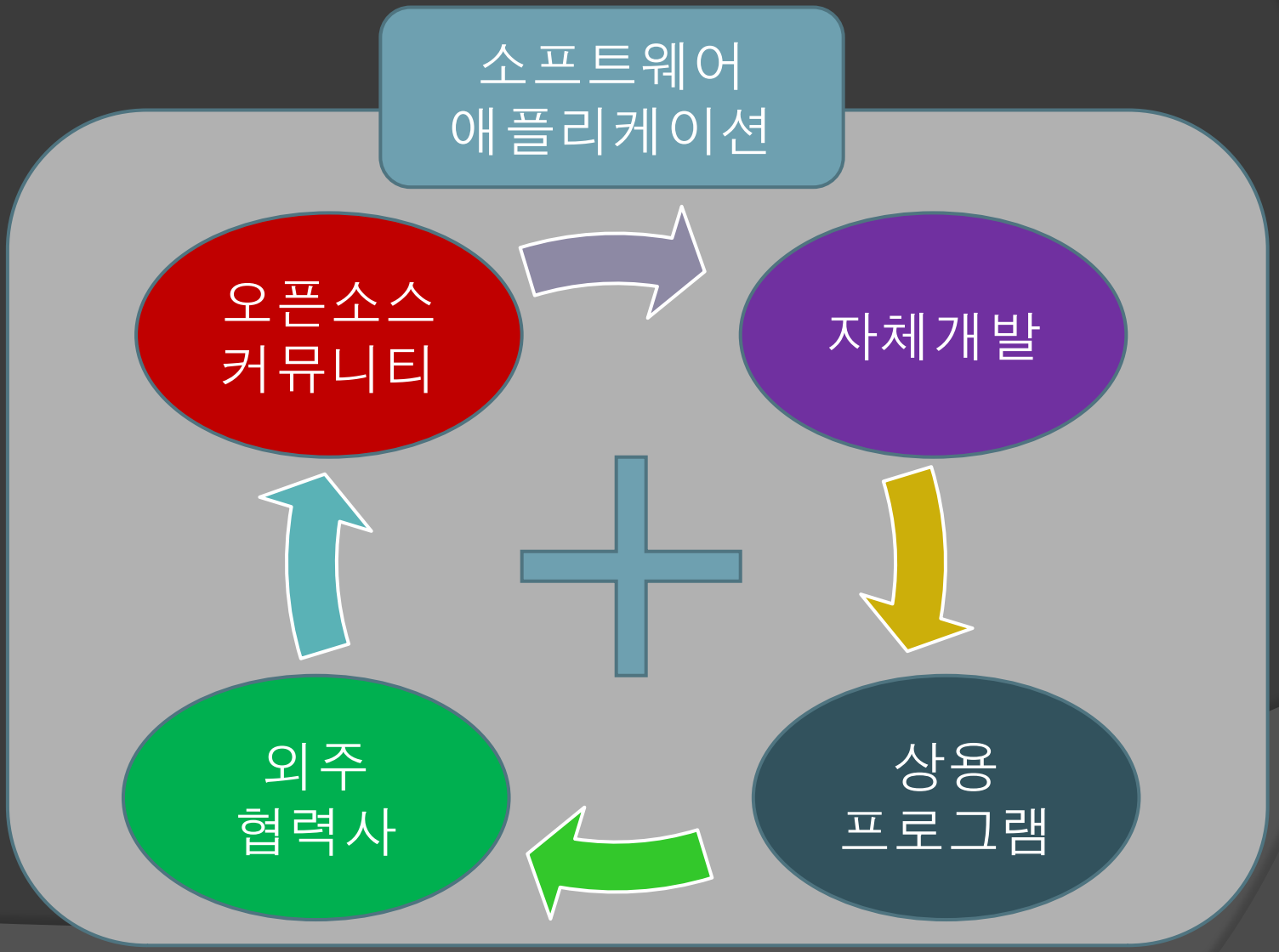
2013 FOSS Con, Korea

공급망에서의 오픈소스 거버넌스

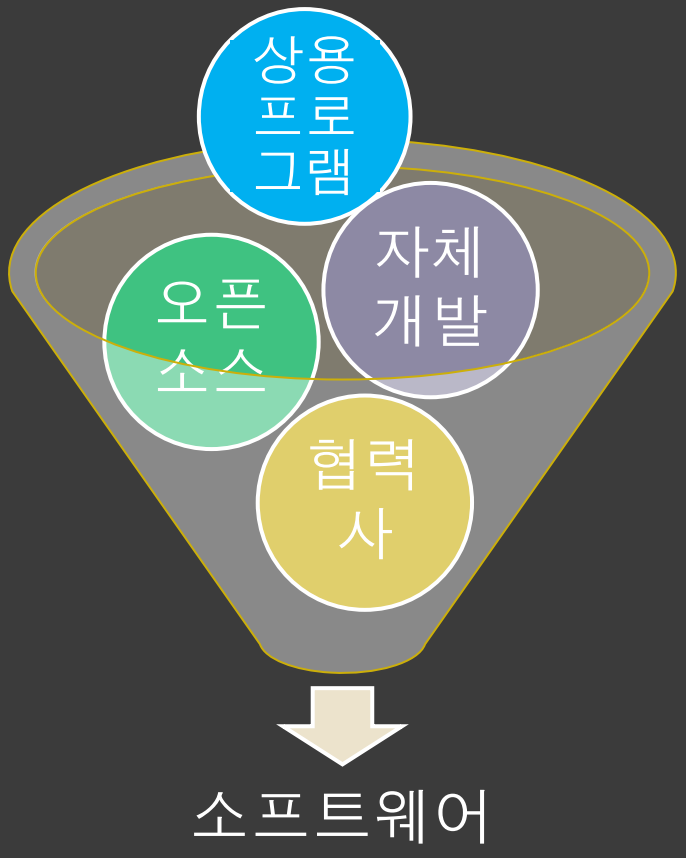
2013년 12월 5일

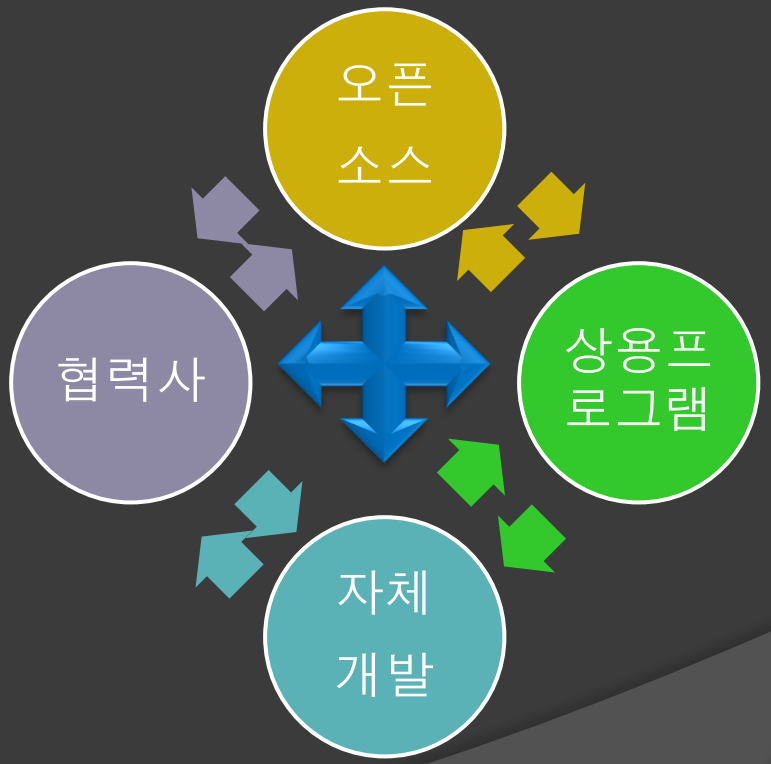
한국 오픈소스SW 법 센터/대표 박종백
블랙덕 소프트웨어 코리아/이사 김병선

소프트웨어 공급망 구성

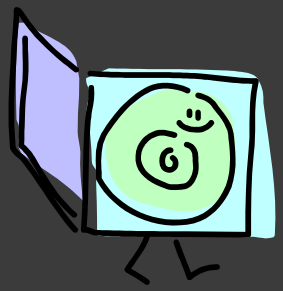


소프트웨어 공급망 구성

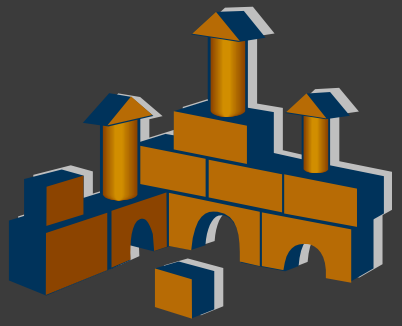




공급망 별 오픈소스 컴플라이언스 범위



오픈소스
소프트웨어



부품제조사

완제품 제조사

유통사

소비자

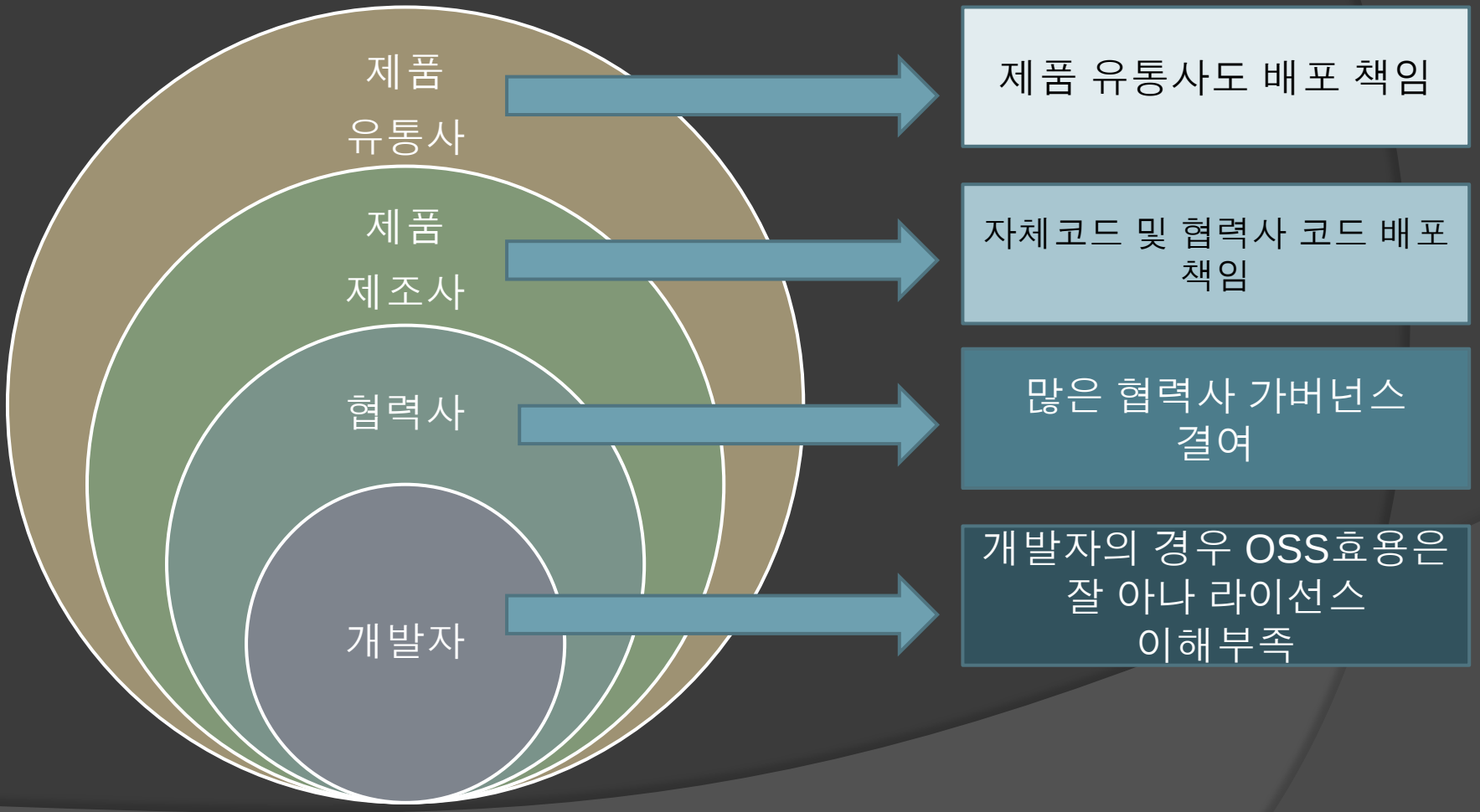
배포의 중요성

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

누가 배포자가 될 것인가

- 최종소비자의 입장에서
  - 오픈소스 소프트웨어가 포함된 제품 제작사
- 라이선스 저작권자 입장에서
  - 오픈소스 소프트웨어의 SUPPLY CHAIN에 있는 모든 관계사
    - 오픈소스 활용한 개발사
    - 오픈소스 활용 부품 공급자
    - 오픈소스 활용 완제품 생산자
    - 오픈소스 활용 제품 판매사

Supply chain 당사자의 책임



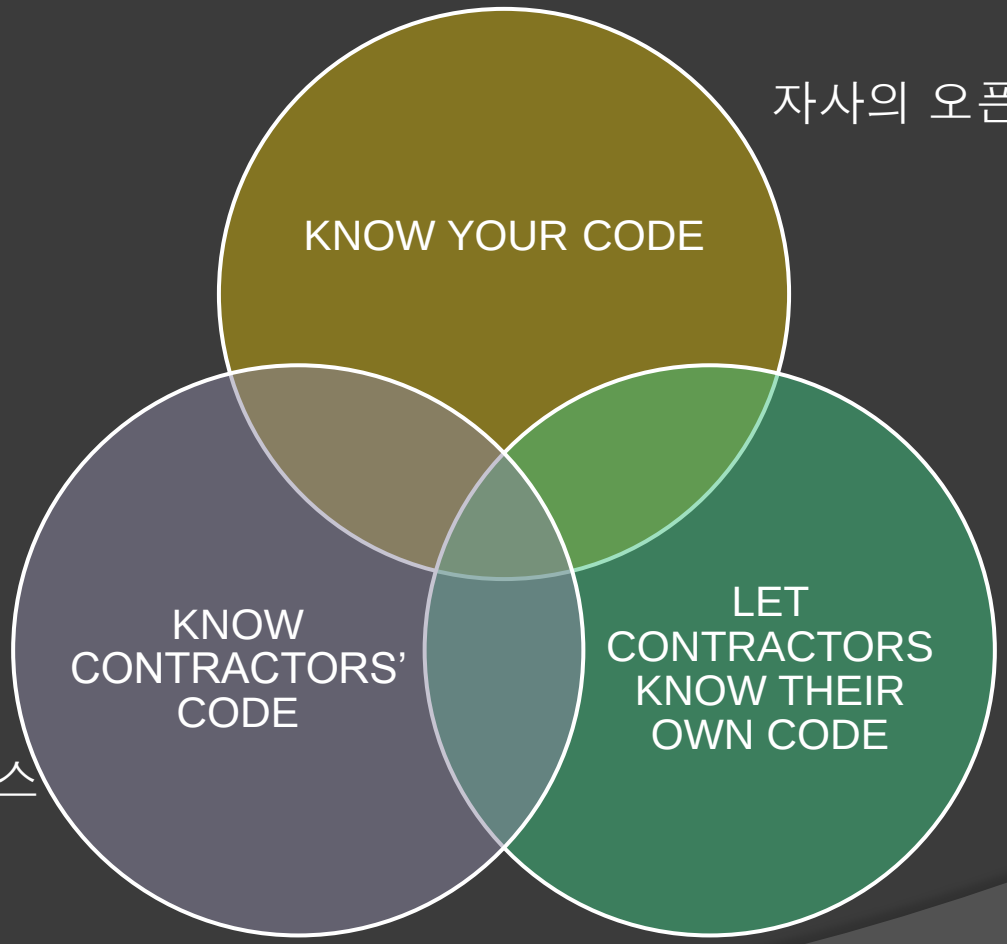
협력사와 계약시 주의사항

- 개발된 소프트웨어에 대한 저작권 및 사용권 귀속여부
- 소프트웨어 사용권만 확보한 경우
  - 유지보수
  - 소프트웨어 역분석
  - 소프트웨어 임치제도 등 확정
- 발주사 면책 및 Indemnity 조항
- Non-competition, Non-disclosure 조항 확인. 특히 경쟁사 관계에서 영업비밀 보호 및 기밀유지
- 품질보증 및 제3자 권리침해 금지

계약을 통한 문제해결의 한계

- 진술및보장의 한계
  - 협력사가 실제로 가버넌스 미구축시 진술보장만으로는 미구축의 위험을 제거하지 못함
- Indemnity 조항의 한계
  - 협력사와 내부관계에서는 Indemnity 조항을 근거로 책임추궁가능하나 저작권자에 대해서는 책임을 짐
  - 협력사의 방어능력이나 지불능력의 미약함으로 자사가 책임추궁을 당함
- OSS 커뮤니티에 대한 노출 및 발언권
  - 소규모 협력사의 경우 국제 커뮤니티와의 대화채널, 능력이 부족함

Supply chain 상 가버넌스의 세가지 축



자사의 오픈소스 가버넌스

협력사 자체의 오픈소스 가버넌스

발주사의 소프트웨어 가버넌스에 대한 검증

협력사 오픈소스 가버넌스 검토 단계

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

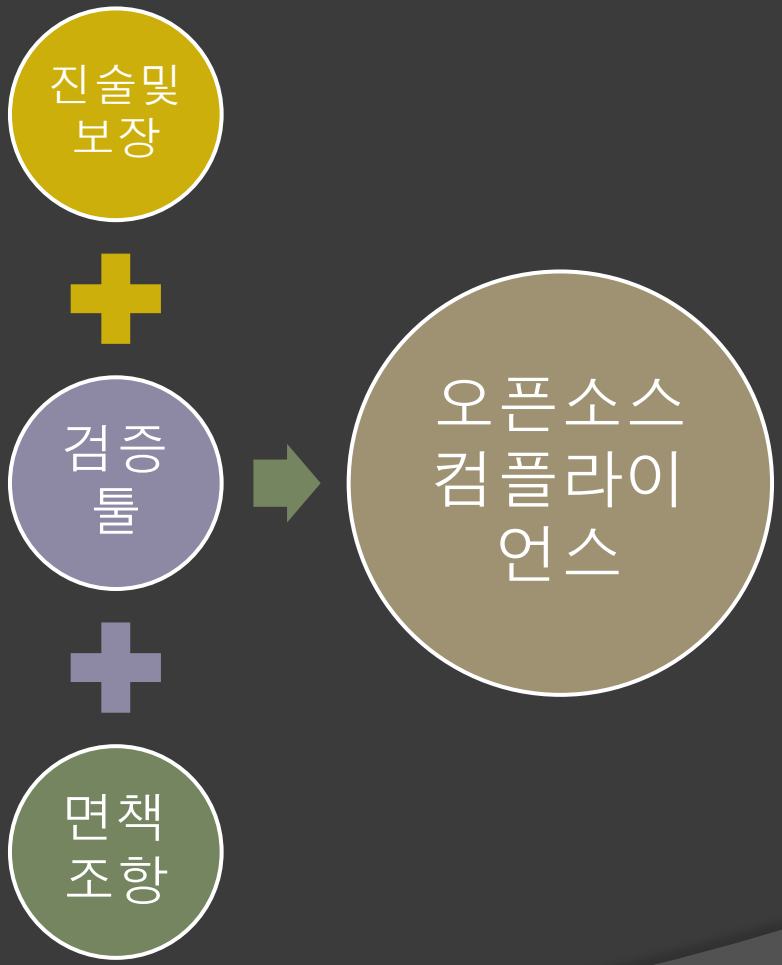
협력사 가버넌스 검토 대상

- FOSS GOVERNANCE 정책의 수립 여부 및 검토
- FOSS COMPLIANCE TOOL의 사용 여부
- FOSS COMPLIANCE OFFICER 역할 및 존재 여부
- FOSS COMPLIANCE 관련 LICENSE NOTICE 공개 여부
- FOSS COMPLIANCE 관련 개발자 교육 여부
- FOSS COMPLIACNE 관련 매뉴얼 및 체크리스트 작성 여부
- FOSS LICENSE 선별 정책의 존재 여부 및 자사 프로젝트와 양립성 여부

협력사 오픈소스 정책 세부내용

- 가버넌스 구축및 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

협력사 컴플라이언스 툴 사용



협력사 오픈소스 라이선스 컴플라이언스

- License Notice
- Source Code Disclosure
- 원저작권자 명시
- 결합방식에 대한 분류
  - Static Linking
  - Dynamic Linking
  - Pipe Line, Call 등 독자적 호출
- 오픈소스 배포 및 컴플라이언스 사이트 운영

SPDX

SPDX®

SOFTWARE PACKAGE DATA EXCHANGE®

- SPDX Group:
  - Linux Foundation의 워킹그룹
  - 20여 개 이상의 소프트웨어, 시스템, 툴 벤더, 컨설턴트 등이 참여
- 표준
  - 소프트웨어 패키지 관련 콤포넌트, 라이선스, copyrights, Chucksum 정보 등을 상호 교환하기 위한 표준
  - Linux Foundation의 오픈 컴플라이언스 프로그램의 핵심
  - www.spdx.org

협력사 오픈소스 컴플라이언스 교육과정

- 오픈소스 가버넌스의 경우 계속적으로 적용되어야 하므로 교육프로그램이 중요
- 본사에서의 컴플라이언스에 대한 교육도 필요하지만 협력사의 개발자 및 경영진을 대상으로 한 교육도 필수적
- 협력사의 경우 촉박한 개발일정으로 인해 컴플라이언스 및 교육과정 소홀히 하기 쉬워
- 용역계약시 충분한 교육과정에 대한 내용을 포함

협력사 체크리스트 작성

- 소프트웨어 구성요소 목록 제출
- 오픈소스 라이선스 목록 작성
  - COPYLEFT 계열 사용시 선승인 요청
- 자사 프로그램을 활용하여 개발할 경우 영업비밀 보호를 위한 조치
- 소스코드 저작권 귀속여부 확정 및 컴파일을 위한 스크립트 제출
- 리눅스 사용관련 주의사항 확인
  - 커널 및 드라이버에 대한 소스코드 제출
- 툴체인의 소스코드 제출

Welte vs. Skype Technologies SA

- SMC라는 인터넷전화기 제조업체가 리눅스를 기반으로 한 펌웨어를 사용하여 인터넷전화기 제조
- 해당 펌웨어는 GPLv2 라이선스 적용
- Skype 독일지사는 이 인터넷전화기를 인터넷을 통해 유통
- 하지만 유통시 GPL license 문구를 명시하고, 사용자에게 source code를 제공하여야 하는 등 GPLv2 의무사항 위반
- 의의: 제조업체 뿐만 아니라 유통업체도 오픈소스 라이선스 위반에 대하여 책임이 있는 점을 판시
- 또한 오픈소스 라이선스 조건을 준수하지 않는 한 오픈소스 소프트웨어가 탑재된 제품의 판매를 중지 명령

라이선스 위반시 법적 효과

- 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

앱의 배포자 구분

앱 개발사	• 개인 • 법인
앱스토어 운영사	• 앱스토어, 올레마켓, 카카오톡 • 올레TV, 티스토어, 삼성APPS 등
통신망 제공사	• SKT, KT, UPLUS • 올레TV 등

애플 앱스토어의 사례

- 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
- 해당앱을 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 지지만 앱스토어의 운영자도 의무사항을 부담하게 되고 앱스토어에서 퇴출될 위험성 발생

온라인 서비스 제공자의 의무

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

저작권법상 온라인서비스제공자의 책임 제한

- 온라인서비스제공자(ISP)가 저작물을 저장 송신 및 중계한 경우에도 특정한 요건을 갖추면 저작권 위반으로 인한 책임을 부담하지 않음
  - 침해행위로부터 직접 금전적 이익을 얻지 않은 경우
  - 침해사실을 알지 못하거나 알게 된 경우 또는 침해가 명백한 경우 즉시 복제, 전송을 중단한 경우 등
- ISP는 자신의 서비스 안에서 침해행위를 모니터하거나 적극적으로 조사할 의무 없음
- 침해사실이 발생할 경우 권리주장자는 즉시 ISP에 해당저작물의 복제, 전송 중단을 요청할 수 있고 이 경우 ISP는 해당 저작물에 대해 즉시 복제, 전송을 중지

앱스토어 운영사의 책임소재 완화를 위한 법률적 검토

- 앱 개발자의 대리인(agent) 주장
- 온라인 유통업자에 대한 면책조항 적용
- 내부적인 indemnity 조항 활용
- 앱개발자를 위한 컴플라이언스 마련
- 앱개발자를 위한 Open Source 라이선스 공지 및 배포 사이트 지침 준수
- 사용자 약관과 주요 오픈소스 라이선스와의 상충 검토 및 수정
- Copyleft 관련 앱이 있는 경우 사용에 있어 추가적인 제한 조항 삭제

애플/구글 앱스토어의 오픈소스

2010년 OpenLogic 분석자료

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

앱스토어 컴플라이언스현황

- 2011년 안드로이드 개발자 컨퍼런스 오픈로직 분석자료
- 분석대상앱
  - 카테고리별 가장 많이 사용되는 유료와 무료앱을 각 10개씩
  - TV에 광고되는 앱
  - 포춘 500기업중 25위 안의 기업들이 발표한 앱
- 분석대상 앱수: 애플 523개, 안드로이드 112개, 총 635개
- 분석대상 앱중 52개앱 아파치 라이선스 활용, 16개앱이 GPL 혹 LGPL 활용
- 오픈소스를 활용한 앱 중 71%가 의무사항 위반
- 일부 오픈소스 앱의 경우 자체 사용자 약관을 적용하여 앱에 대한 저작권 주장
- 가장 많이 사용되고 가장 규모가 큰 기업들이 발표한 앱을 분석대상으로 하였다는 점에서 오픈소스 컴플라이언스 미비로 인해 서비스가 중지될 경우 심각한 경제적 파장 초래 가능