2nd FOSSLight Community Day

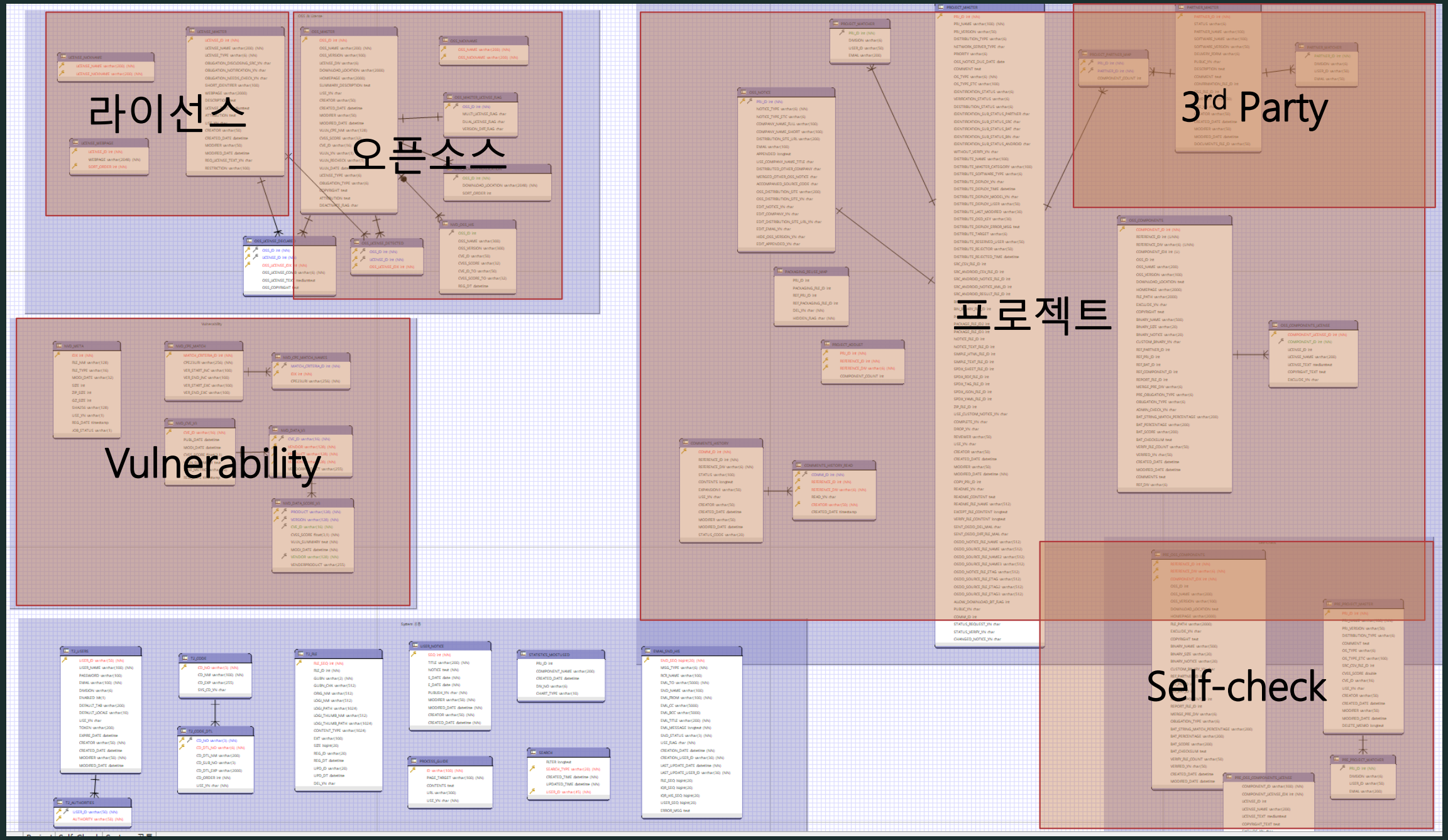
FOSSLight Hub ERD

㈜ 씽크트리 윤성원

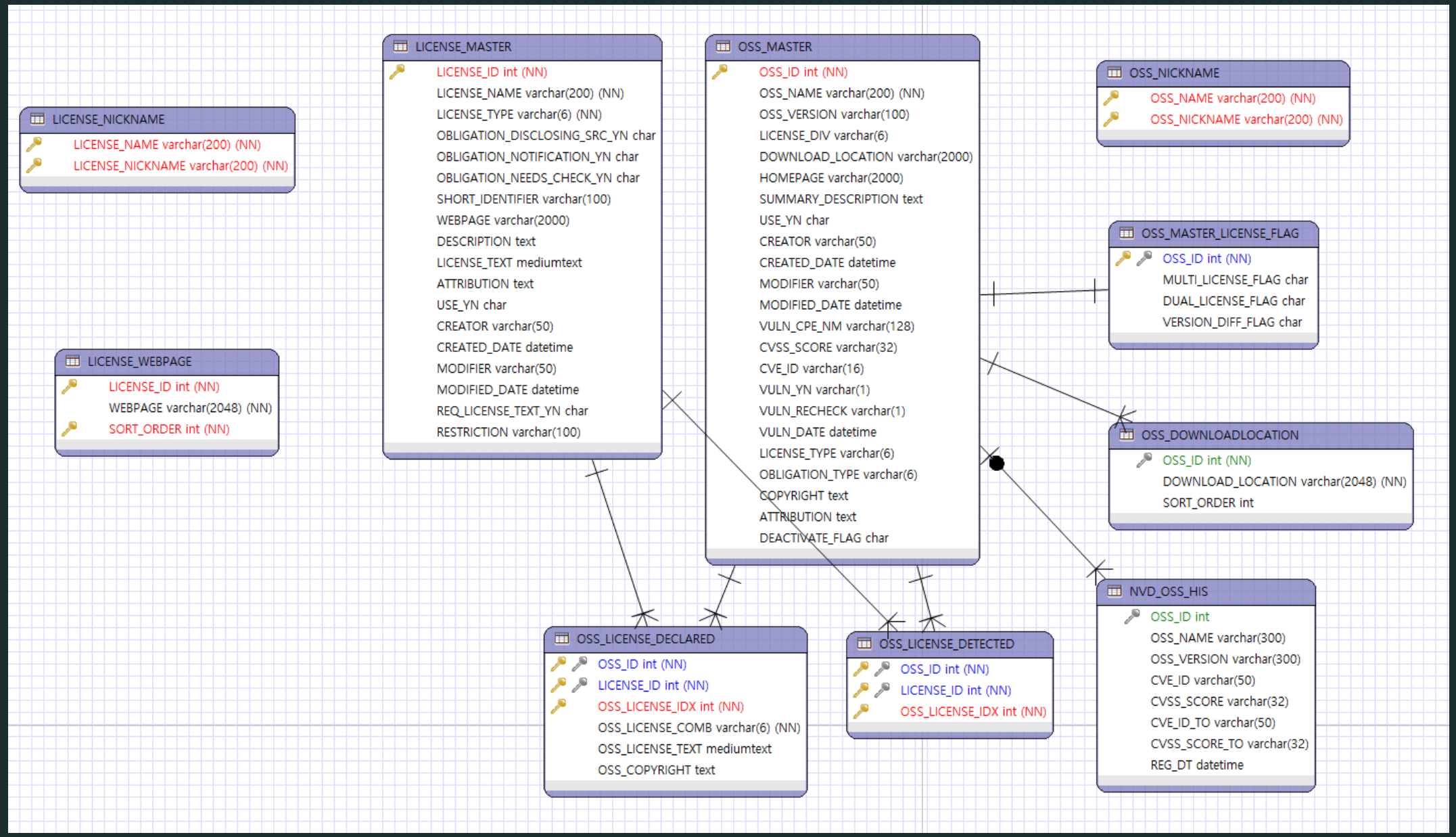
Contents

- Open Source & License
- Open Source Compliance (Project)
- Vulnerability (NVD Data feeds)
- Database Extension

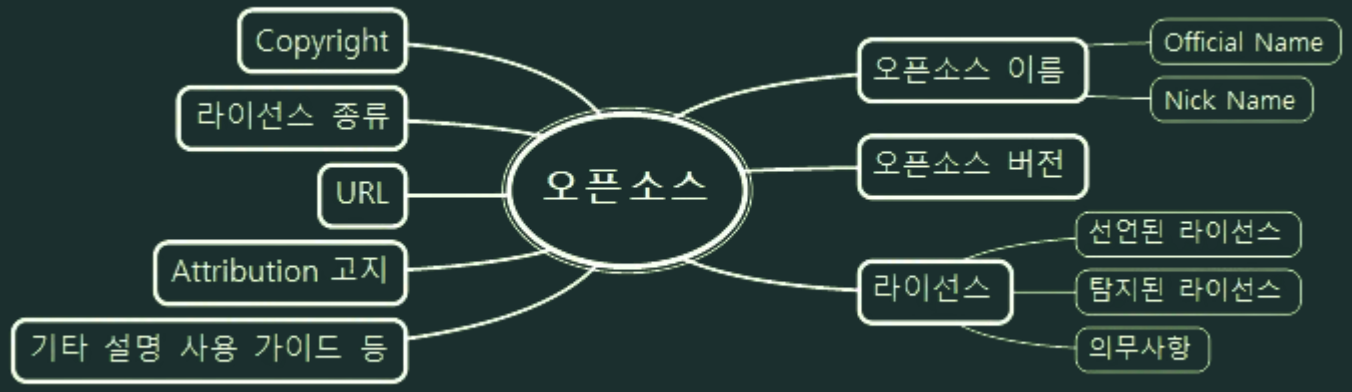
FOSSLight Hub ERD



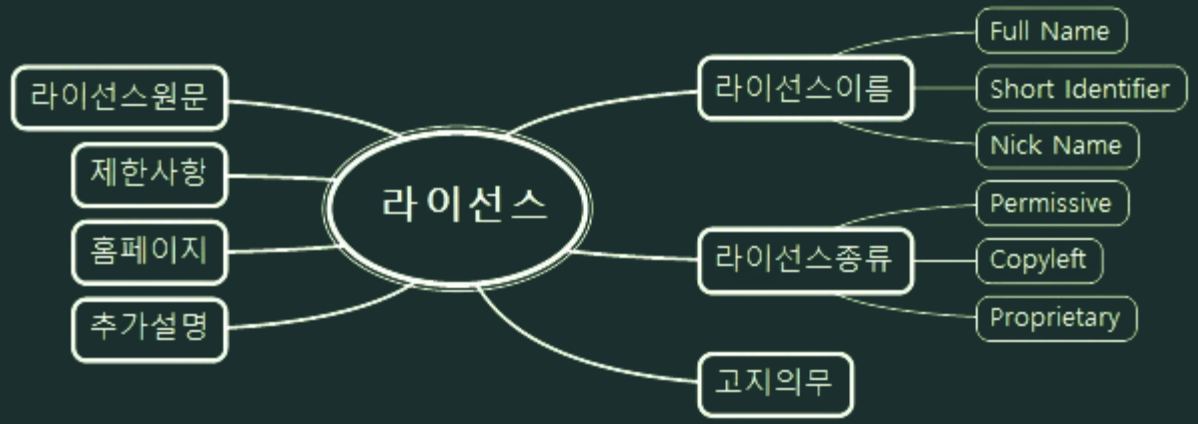
Open Source & License



Open Source & License

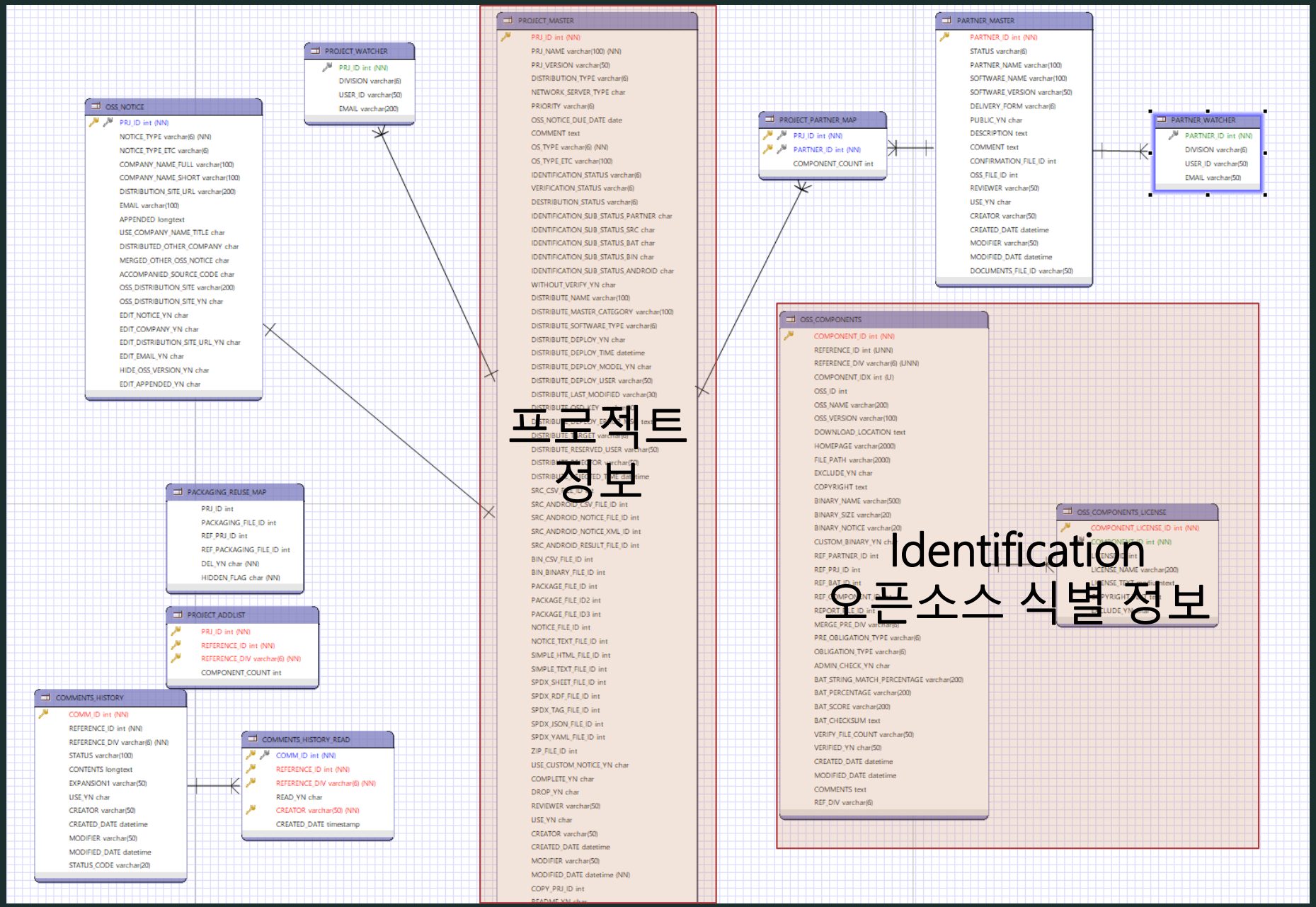


- PK = OSS ID = (OSS Name + OSS Version)
- 오픈소스 이름은 버전과 무관하게 유니크
- 닉네임도 유니크
- 닉네임도 정식 명칭과 동일하게 동작

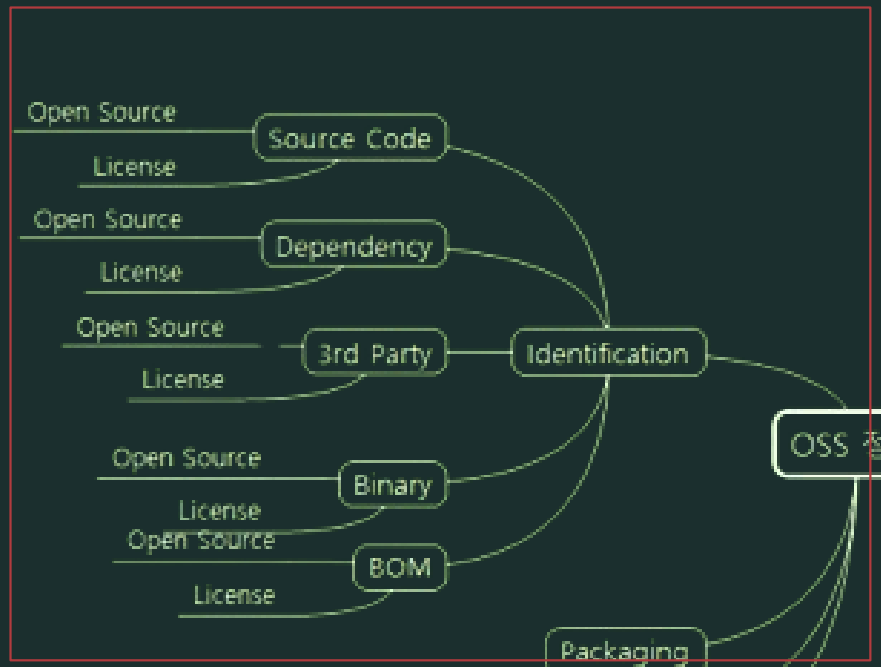


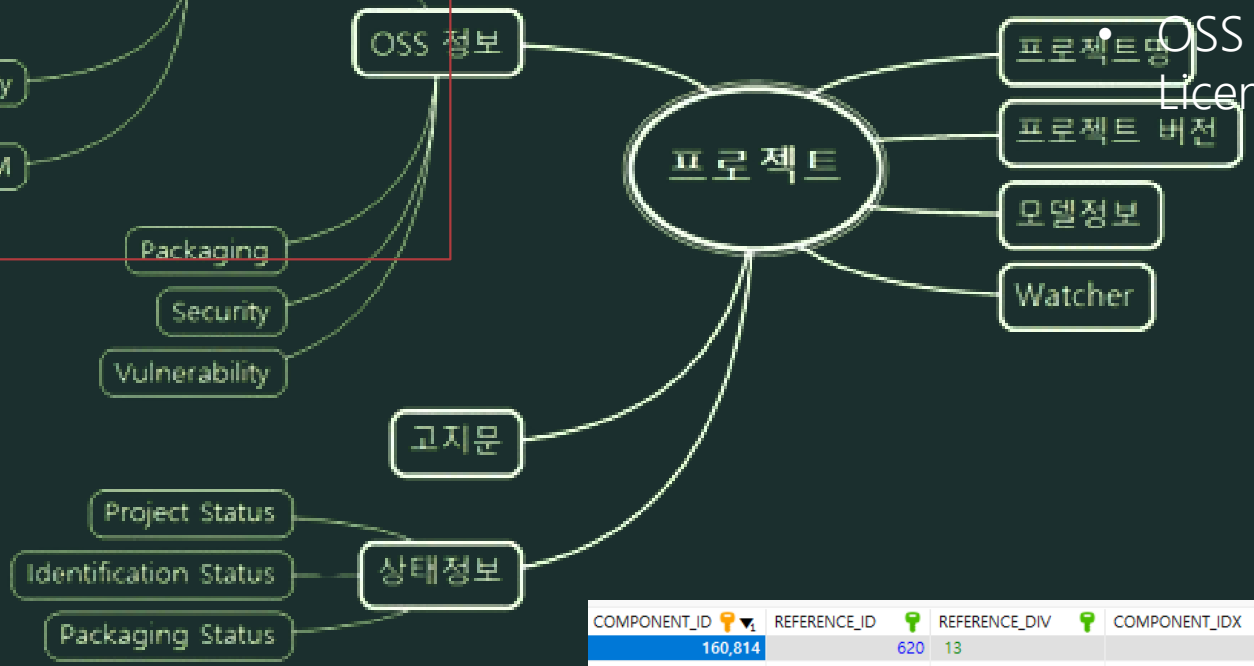
- Full Name = Sort Identifier = Nick Name
- Sort Identifier가 설정된 경우 우선 표시

Open Source Compliance (Project)



Open Source Compliance (Project)



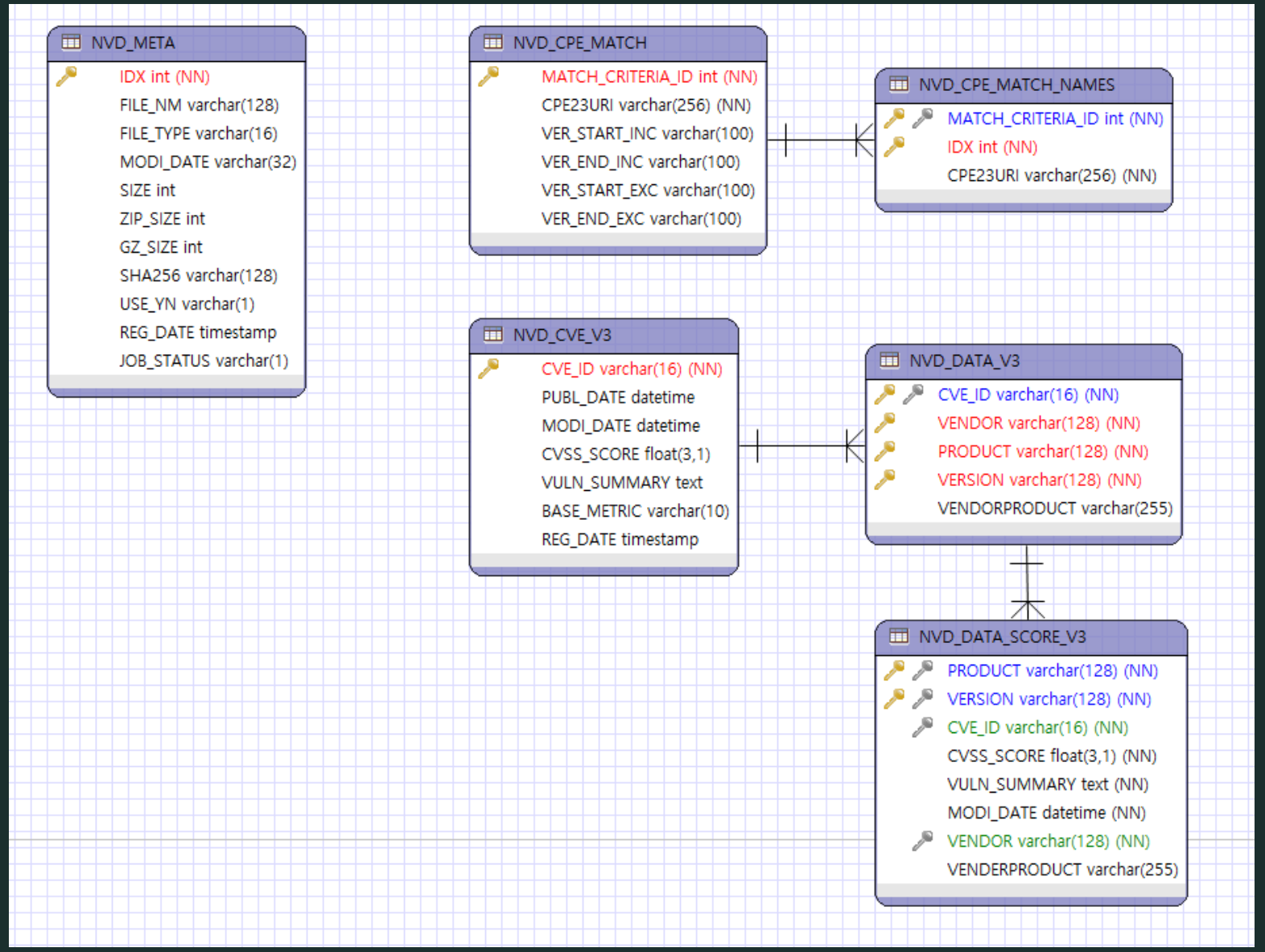


- PK = PRJ ID = (Name + Version)
- 프로젝트 정보와 오픈소스 식별 정보 크게 2개의 Table로 관리
- OSS 식별 정보 (OSS_COMPONENTS)
  - 각 프로젝트별(3rd party 공통) SRC, DEP, BOM 등 모든 유형별 오픈소스 정보를 하나로 관리
  - PK = COMPONENT_ID
    = (REFERENCE_ID + REFERENCE_DIV + COMPONENT_IDX)

- OSS 식별 정보의 라이선스는 모드 Multi License로 저장 및 동작

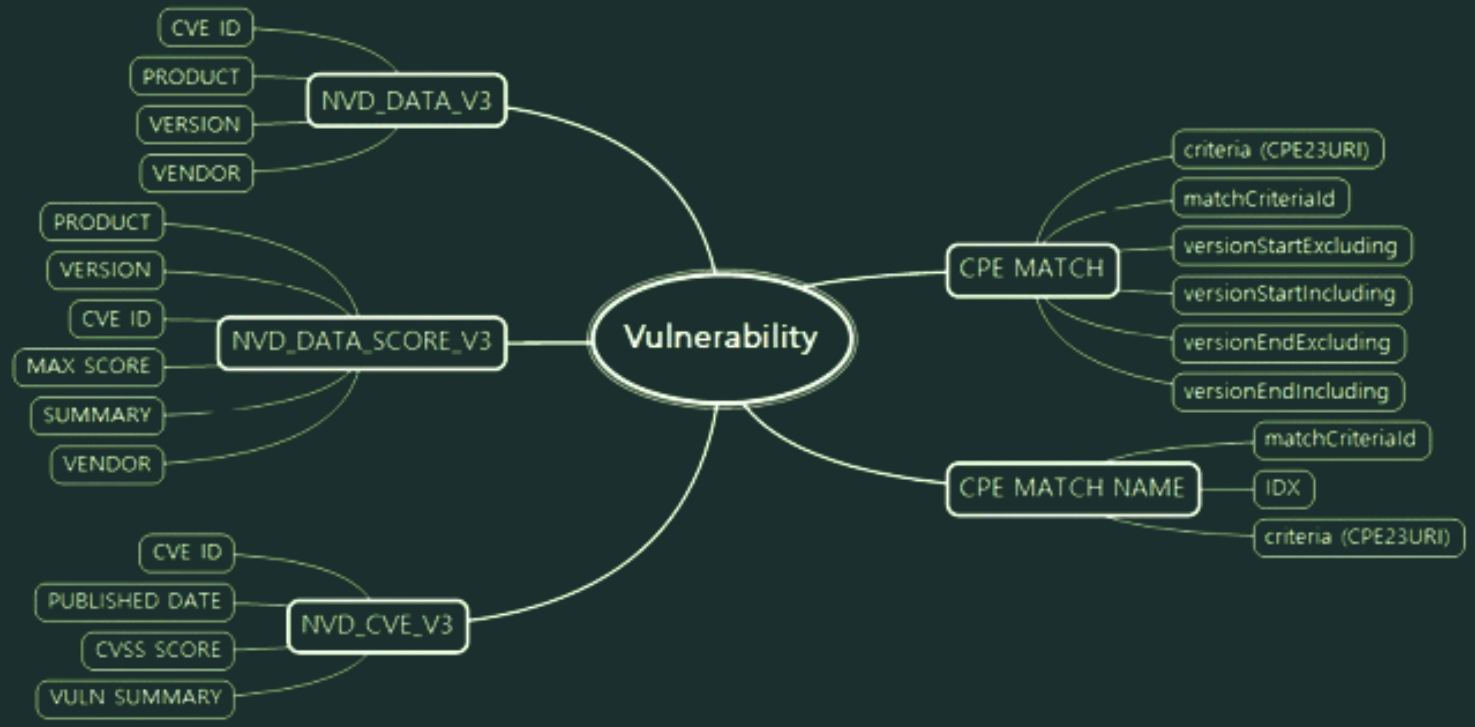
COMPONENT_ID	REFERENCE_ID	REFERENCE_DIV	COMPONENT_IDX	OSS_ID	OSS_NAME	OSS_VERSION	DOWNLOAD_LOCATION
160,814	620	13	2	6,718	cairo	1.4.12	http://cairographics.org/relea
160,813	620	13	1	2,121	Apache Ant	1.6.5	http://archive.apache.org/dis
160,810	620	10	2	2,121	Apache Ant	1.6.5	http://archive.apache.org/dis
160,809	620	10	1	1	cairo	1.4.12	http://cairographics.org/relea
160,808	618	13	1	34,667	wrong name	1.0	https://github.com/lodash/lo
160,806	618	11	1	34,667	wrong name	1.0	https://github.com/lodash/lo
160,805	605	15	1	34,732	asdfasdf	123	http://www.google.com
160,804	605	16	1	34,732	asdfasdf	1	http://www.google.com
160,803	605	11	1	34,732	zxcvzxcv	123	http://www.google.com

Vulnerability (NVD Data feeds)



Vulnerability (NVD Data feeds)

- NVD Data 는 CPE 정보와 CVE 정보로 구분할 수 있음
- CPE
  - MATCH : Criteria Id 에 해당하는 Version Range 정보
  - MATCH NAME : 대상에 포함되는 Version정보를 포함한 CPE23URI
- CVE
  - CVE_V3 : CVE정보 (CVE_ID, Score, Summary 등)
  - CVE_DATA_V3 : CVE_ID에 포함되는 오픈소스 정보
  - SCORE_V3 : 오픈소스 기준 MAX Score 그에 해당하는 CVE_ID




```
▼ matchString {8}
    matchCriteriaId : 2E9D7615-B1E6-4A06-B709-1709B0F9A0DE
    criteria : cpe:2.3:a:apple:itunes:*:-:mac:*:*:*:*:*
    versionEndIncluding : 9.0.3
    lastModified : 2019-06-17T09:16:33.960
    cpeLastModified : 2019-07-22T16:37:38.133
    created : 2019-06-17T09:16:33.960
    status : Active
  ▼ matches [38]
    ▼ 0 {2}
        cpeName : cpe:2.3:a:apple:itunes:4.0.0:-:mac:*:*:*:*:*
        cpeNameId : 80B46D10-B35E-4149-A084-E42B4DD58ECC
    ▼ 1 {2}
        cpeName : cpe:2.3:a:apple:itunes:4.0.1:-:mac:*:*:*:*:*
        cpeNameId : ABC8FECD-38B7-4936-969B-C7941168ED15
    ▼ 2 {2}
        cpeName : cpe:2.3:a:apple:itunes:4.1.0:-:mac:*:*:*:*:*
        cpeNameId : F71E6009-DA0A-43CF-9234-B6A1A7611CD4
    ▼ 3 {2}
```

Database Extension

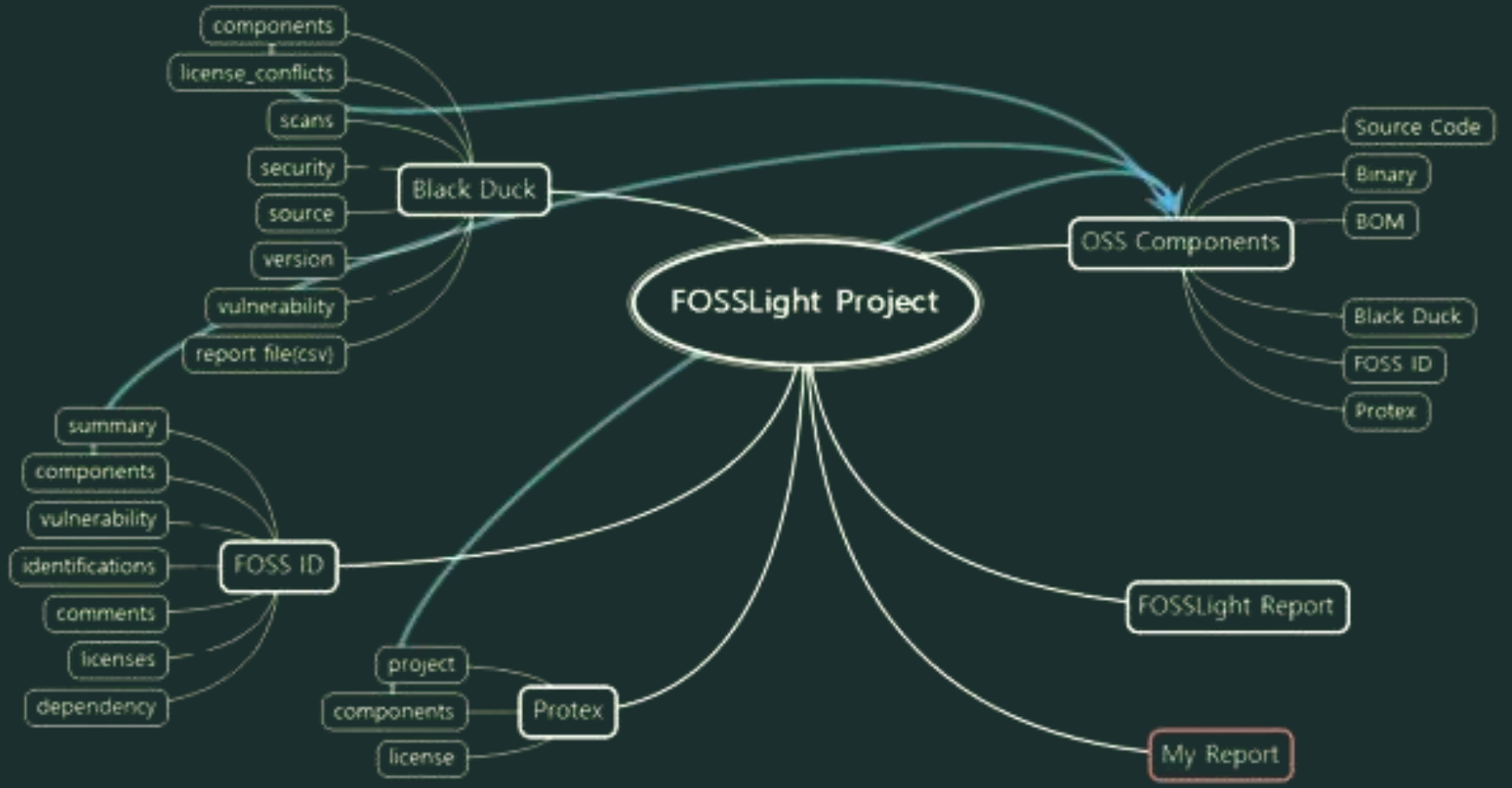
- 이미 사용중인 상용 분석툴SW를 연동
- 추가적으로 관리하고 싶은 정보가 있다
- 초기 Data의 설정 또는 선택 값을 변경, 추가 하고 싶다
- 프로세스를 수정하면서 이메일을 추가하거나, 일부는 사용하고 싶지 않다

- 기존에 테이블에 필드를 추가할 것인가? 별도 테이블로 분리 할 것인가 검토 할 것 (FOSSLight 업그레이드 고려)

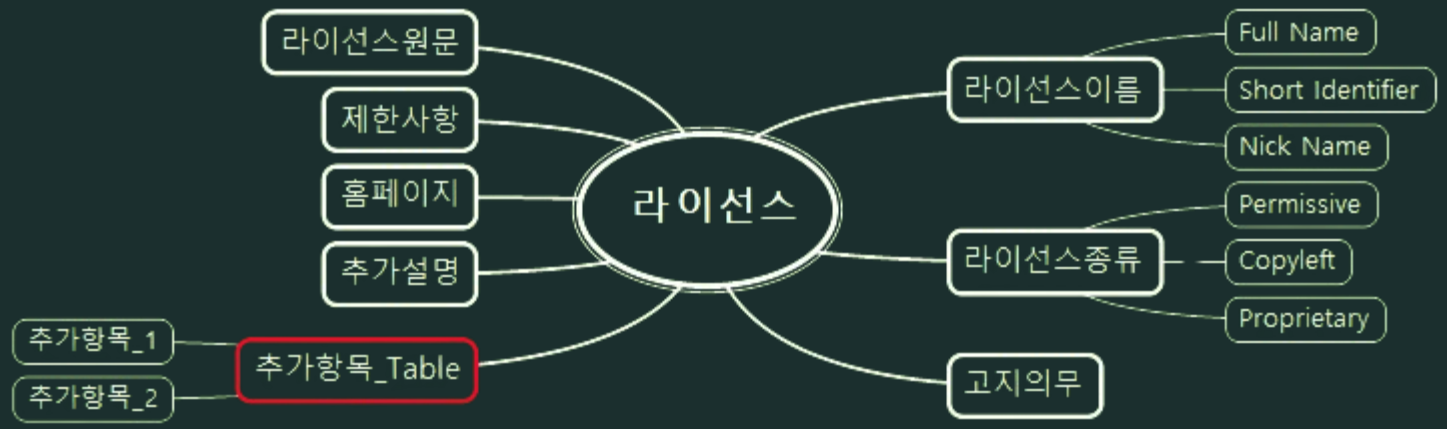
- FOSSLight Hub에서 기본적으로 제공되는 선택 항목은 모두 공통 코드로 관리하고 있음, 기존 항목에 Item을 추가하고자 하는 경우 코드 관리를 먼저 확인
- 이메일 추가는 가급적 기존 이메일 발송 class를 복사해서 별도의 이메일 발송용 Class를 작성하자
- 상용 분석툴을 연동하는 경우 상용 분석툴 레포트 결과를 별도의 테이블에 저장하고 Identification에 저장하는 것을 권고

Database Extension (상용 분석툴 연동시 고려사항)

- 상용 SW 분석툴을 연동하는 경우, 검증 진행중에 분석툴의 정보가 변경되어도 영향이 없도록, 요청시점의 취득한 정보를 별도의 DB로 저장해둘 것을 권장
- 상용 SW 분석툴에서 식별된 오픈소스를 변경할 수 있게 할 것인가?
- Version, License 정보 등 미식 정보에 대해서는 고려해야 함



Database Extension (필드 추가 시 고려사항)



- 예를 들어
  라이선스 관리 화면에서 항목을 추가하는 경우, FOSSLight Hub의 LICENSE_MASTER table에 추가할 것인지 별도의 Table을 추가할 것인지 검토
  이후 FOSSLight Hub upgrade를 고려한다면 별도의 Table로 Add-on하는 것을 권장
- 다만, 추가항목에 대한 Data 조회, 수정 등의 처리를 수행할 때 기존 로직에 어떻게 추가해야 하는가? (RequestMapping, Value Object, Transactional 등 충분히 검토 후에 결정)

Q&A