2024. 05

요약본

SW 공급망 보안 가이드라인

SW 공급망 보안 국제동향 및 SBOM 활용사례

국가정보원
과학기술정보통신부
대통령직속 디지털플랫폼정부위원회

요약본

SW 공급망 보안 가이드라인 v 1.0

SW 공급망 보안 국제동향 및
SBOM 활용사례

2024. 05

국가정보원 과학기술정보통신부 대통령직속 디지털플랫폼정부위원회

Contents

요약본은 공공기관 및 기업 관계자들이 짧은 시간 내에 SW 공급망 보안 가이드라인의 주요 내용을 쉽게 파악할 수 있도록 지원하기 위하여 마련되었습니다.

또한 요약본은 전체본의 목차를 그대로 따르지 않고, 전체본 제2장 제3절의 SBOM 기반의 SW 공급망 보안을 분리하여, SBOM 실증결과, 기업지원 시설 등과 함께 별도의 장으로 구성하여 다양한 계층의 독자들이 조금이라도 더 쉽게 이해할 수 있도록 지원하기 위해 노력하였습니다.

특히, SW 공급망 보안 관련 상세한 내용보다는 빠른 시간 내에 개념 중심으로 SW 공급망 보안에 대한 이해가 필요한 정책 결정자 및 기업 경영진들에게 유용할 것으로 보입니다.

본 요약본을 통해 SW 공급망 보안에 대한 개념을 이해한 후 전체본을 읽으면서 세부적인 내용을 파악하는 방식으로 활용해도 효율적일 것입니다.

정부는 다양한 분야의 독자들의 제언을 수용하여 SW 공급망 보안 가이드라인을 계속해서 발전시켜 나가겠습니다.

국가정보원 과학기술정보통신부 대통령직속 디지털플랫폼정부위원회

제1장

추진 배경

(환경변화) 사람과 사물(공간·생물·정보·비즈니스 등)이 물리·가상 공간의 경계 없이 서로 유기적으로 연결되어 소통하고 상호 작용하는 초연결사회 도래

- **(SW 생산의 분업화)** 디지털 제품 및 서비스에 대한 SW 부품(코드) 공급의 분업화로 관리 책임이 복잡해지고, 제품 및 서비스 무결성에 대한 신뢰 하락

> SW 공급망은 최종 SW 제품을 생산하는 사람, 장치, 시스템의 집합을 말함. 이는 개발자가 코드를 작성할 때부터 해당 코드가 제품으로 생산된 후, 사용자 시스템에서 실행되는 과정까지 일어나는 모든 일을 의미함

- **(공개 SW에 대한 사이버위협)** 디지털 제품 및 서비스는 대부분 자체 개발 SW 외에 다양한 공개 SW, 제3자 개발 SW 등 외부 SW를 포함, 특히 악성코드 및 보안취약점의 전파가 쉬운 공개 SW에 대한 사이버 위협 증가

(SW 공급망 보안 필요성) 공급망 공격은 공개 SW의 보안취약점 및 악성코드를 악용한 것으로 피해가 광범위하고 지속적인 특징을 나타냄

- **(큰 피해규모)** SolarWinds('20년), Log4j('21년) 및 Kaseya('22년)와 같이 대형 SW 공급망 공격이 매해 발생하고 있어 빠른 대응 체계 구축 필요
- **(파급효과)** 고객의 소스코드를 검증하는 회사인 Codecov는 리포지토리 인증 정보가 유출되어 2차 공격의 파급을 가늠하기 어려움('21년)
- **(지속적 피해)** 공개 SW로 널리 활용된 Log4j의 경우 보안취약점 삭제·업데이트 등에 10년이 소요될 것으로 예측(美 사이버보안검토위원회, '22년)

사례	사고 내용 및 피해 현황
SolarWinds (2020년)	러시아 기반 해킹 그룹의 공격으로 IT SW 공급사의 SW 개발 환경 및 배포 시스템이 해킹되어 18,000개 이상의 기관이 피해를 입음
Log4Shell (2021년)	Log4j의 제로데이 보안취약점과 공개된 개념 증명 코드를 악용하여 악성코드를 심고, 전 세계 취약 서버를 대상으로 대량의 해킹 공격 발생
Kaseya (2022년)	클라우드 기반 IT 원격 관리 솔루션 서버를 해킹하고, 업데이트 파일로 위장한 랜섬웨어를 고객사에 배포. 17개국 1,500여 조직이 피해

(주요국 정책동향) 미국, 유럽 등은 SW 공급망 공격에 체계적으로 대응하기 위해 SW 구성요소 명세서(SBOM, SW Bill of Materials) 도입 등 제도화 추진

- **(미국)** 바이든 정부 행정명령(EO 14028, '21.5월)을 통해 연방정부에 납품되는 SW의 SBOM 제출을 의무화하였고,
  - 관리예산처(OMB)는 '안전한 정부를 위한 SW 공급망 보안 강화 지침'과 '행정 부서 및 기관장을 위한 각서(Memorandum)'를 발표('22.9월)

> **OMB '행정 부서 및 기관장을 위한 각서(M-22-18)' 주요 내용**
> 연방정부에 SW를 납품하는 공급자에게 미국 국가기술표준원(NIST)[1]의 안전한 SW 개발 체계(SSDF)[2]를 준수했음을 선언하는 '자체증명서(Self-attestation Form)[3]'를 함께 제출토록 함
> - 자체 증명 항목 : 안전한 개발 환경 구축, 자동화된 소스코드 출처 관리, 지속적 취약성 검사 등을 수행
> - 이외에도 안전한 SW 개발체계 적합성을 입증하는 증거를 별도로 요구할 수 있음,
>
> 제출은 온라인(softwaresecurity.cisa.gov) 또는 이메일로 접수

- **(유럽)** EU는 역내에 유통되는 디지털기기의 SBOM 제출을 의무화하는 사이버 복원력 법(Cyber Resilience Act, CRA) 제정안을 발의('22.9월, EU 집행위원회)
  - '24.3월, 유럽의회는 CRA 내용을 확정·승인하였으며, 향후 이사회(Council) 승인을 거쳐 최종 법률안의 효력 발생은 2026년 하반기로 예상

(시사점) SW 공급망 보안에서 공개 SW의 보안취약점 관리가 매우 중요하며, 효과적인 보안취약점 관리 방안으로 SBOM이 대두되고 있음

- 지난 수년간 SW 공급망 공격은 국제적인 논의의 중심이 되고 있으며, 미국, 유럽 등 주요국을 중심으로 SW 공급망 보안 제도화 추진 중
  - 우리나라도 SBOM 기반 SW 공급망 보안 체계 확산을 위해 SW 공급망 전 단계에서 SBOM을 원활하게 유통할 수 있는 관리 체계 마련 필요
  - 해외 주요국의 SW 공급망 보안 정책을 빠르게 분석하고 선제적으로 대응하여 국내 기업의 해외 진출 시 무역장벽 극복 지원 필요

1) NIST : National Institute of Standards and Technology

2) SSDF : Secure Software Development Framework

3) 증명(Attestation) 이란 문서의 진위를 법적으로 인정하고, 적절한 프로세스를 따랐다는 것을 입증하는 절차로써, 문서의 내용에 구속된 사람들이 적절하게 행동했음을 확인하기 위해 서명하고, 제삼의 검증기관(3rd Party Organization)을 통해 공증하는 것 등을 의미함

제2장

SW 공급망 위험관리 방안

제1절 공급망 사이버보안 위험관리 체계 구축 방안

(공급망 사이버보안 위험관리 개요, C-SCRM[4]) 공급망 전체에서 사이버보안 위험을 관리하고 적절한 대응 정책 및 전략 등을 개발하기 위한 체계적 프로세스

- 공급망의 사이버보안 위험은 공급자(개발사 및 유통사), 공급망(개발 및 업데이트 전송로), 제품 및 서비스에서 발생할 수 있는 피해와 침해 가능성을 의미
- 공급망의 사이버보안 위험은 공급망 전체에 걸쳐 있는 제품 및 서비스의 보안취약점과 노출을 악용하는 위협에서 발생

(공급망 사이버보안 위험관리 활동) NIST는 C-SCRM을 통해 기업 또는 기관이 공급망에서 사이버보안 위험을 관리하는데 도움이 되는 활동들을 제시

- C-SCRM은 설계, 개발, 제조, 구매, 배송, 통합, 운영 및 유지보수, 폐기 등 전체 'SW 개발 생명주기(SDLC)'에 걸친 활동을 포괄하므로 공급망 전반의 사이버보안 위험을 해결하려면 C-SCRM이 SDLC 내에 통합되어야 함
  - 또한, 정보보안 및 개인정보보호, 시스템 개발자 및 엔지니어, 인수, 조달, 법무, 인사(HR) 등 기업 내 다양한 이해관계자 그룹이 함께 참여해야 함
- 공급망 내에서는 적대적(Adversarial) 또는 비적대적 이유로 다양한 사이버 위협이 발생할 수 있으며, 이를 해결하기 위해 C-SCRM을 전사적 위험관리 체계에 통합해야 함
  - 또한, 기업 전반의 위험을 관리하기 위해서는 전사적, 프로세스, 운영 수준 모델을 포함하는 '다단계 전사적 위험관리'가 필요
- '다단계 전사적 위험관리'에서 C-SCRM 활동은 아래와 같은 세 가지 레벨로 구분하여 수행
  - 레벨-1(전사) : 전반적인 C-SCRM 전략, 정책, 구현 계획을 통해 전사적인 C-SCRM으로 관리되는 데 필요한 기조, 거버넌스 구조, 경계를 설정
  - 레벨-2(프로세스) : 레벨-1에서 결정한 전사적인 상황과 방향을 가정하고, 이를 특정한 미션(Mission) 및 비즈니스의 프로세스에 맞게 조정

4) 美 NIST 800-161r1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organization

– 레벨–3(운영) : C–SCRM 계획은 정보시스템이 비즈니스·기능·기술 요구사항을 충족하고, 적절하게 조정된 통제를 포함하는지를 결정하기 위한 기반을 제공

다단계 전사적 위험관리(C–SCRM) 개요

(SW 개발·운영 환경의 공급망 보안 체계 구축 방안) SW 공급망 전체의 사이버보안 위험을 관리하기 위해 공급망 참여자(개발사, 공급사, 운영사)들은 SW 공급망에서 안전한 SW 개발·운영을 위한 각자의 역할을 완수해야 함

• 미국의 지속적인 보안 프레임워크(ESF, Enduring Security Framework[5])는 안전한 SW 개발·운용을 위한 공급망 참여자들의 보안활동을 제시('22. 8월)

개발사 SW의 설계와 구현, 검증 등 개발 단계에서 보안 활동을 통해 보안취약점을 최소화해야 할 뿐만 아니라, SW에 포함된 라이브러리와 빌드 및 배포 체계의 보안성을 확보하여야 함

공급사 보안 요구사항 충족 확인, 타사 SW의 검증, 실행 파일의 테스트를 통해 SW 제품의 보안을 검증하고, 보안취약점을 발견했을 때는 고객(운영)사에 이를 알리고, 보안취약점에 대응해야 함

운영사 보안 요구사항과 공급망 위험관리(SCRM) 요구사항을 정의하고, 이에 따라 SW 인수테스트를 진행하며, 제품 적용 및 생명주기 관리에 필요한 보안 및 공급망 위험관리 대책을 구현해야 함

5) ESF는 CISA, NSA 등이 참여, 주요 인프라 및 국가 안보 시스템에 대한 위험을 해결하기 위한 민관 파트너십, 다만, 국내에 적용할 때는 미국 환경과 다소 차이가 있을 수 있음을 고려할 필요

(안전한 SW 개발 체계의 활용) SW 공급망 참여자들은 공급망 보안활동을 수행할 때 NIST의 '안전한 SW 개발체계(SSDF[6])'를 활용할 수 있음

- 인력과 프로세스, 기술이 안전한 SW 개발을 수행할 수 있도록 준비되어 있는지 확인
- SW의 모든 구성요소가 변조되거나 비인가 접근이 이루어지지 않도록 보호하며, SW를 출시할 때 보안취약점을 최소화하여 보안이 잘 갖춰진 SW를 개발
- 출시된 SW에 남아있는 보안취약점을 파악하고 해당 보안취약점을 해결하기 위해 적절히 대응하고 향후 유사한 보안취약점이 발생하지 않도록 예방

[SSDF의 주요 특징]

① 안전한 SW 개발에 관한 지식이 없어도 이해할 수 있는 공통 언어를 제공하여 조직 내·외부 이해관계자*가 소통하는 데 도움을 줌

* 조직 내부의 사업 책임자, SW 개발자, 프로젝트 관리자, 사이버보안 전문가, IT 운영자, 보안취약점이 적은 SW 확보가 필요한 조직 외부의 SW 구매자 등

② 사용하는 SDLC 모델과 관계없이 적용할 수 있으며, 기술, 플랫폼, 프로그래밍 언어, 운영 환경과 관계없이 모든 유형의 SW 개발에 사용할 수 있음

- SSDF는 위의 권고를 충족하는 방법으로 조직 준비(Prepare the Organization, PO), SW 보호(Protect the Software, PS), 보안성 높은 SW 개발(Produce Well-Secured Software, PW), 보안취약점 대응(Respond to Vulnerabilities, RV) 등 각 원칙에 관한 자세한 설명과 필요한 과업(Task)을 제시하였음

제2절 SW 구성요소의 신뢰성 확보 방안

(SW 구성요소 명세서, SBOM) 대표적인 SW 공급망 공격 사례인 SolarWinds 및 Log4j 공격이 큰 피해를 낳으면서, SW에 어떤 구성요소가 존재하는지 신속하게 파악하고, 위험에 대처하기 위한 도구로 SBOM 활용이 부각

- SW 제작 시에 외부 라이브러리나 공개 SW를 포함하여 SW 공급망이 복잡해지고, 보안취약점이 증가함에 따라 이를 추적하고 관리해야 할 필요성이 대두

6) Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities, NIST SP 800-218(2022년 2월)

(SBOM 최소요건) 美 NTIA(National Telecommunications and Information Administration)는 SBOM을 SW 구성요소의 투명성 강화 방안으로 사용하기 위해 최소요건을 제시

- SBOM의 최소요건은 ①데이터 필드(Data Fields), ②자동화 지원(Automation support), ③관행 및 프로세스(Practices and processes) 영역을 포함
  - 데이터 필드는 '공급자명', '타임스탬프', '저작권자', '구성요소명', '버전', '고유식별자', '종속성 관계' 총 7개의 기본항목을 포함
  - 자동화 지원을 위해 SBOM은 컴퓨터 시스템 간 교환이 용이하도록 정해진 형식에 맞춰야 하며, 3가지(SPDX, CycloneDX, SWID) 포맷을 활용하는 것을 SBOM 공유 및 교환을 위한 자동화 요구사항으로 정의
  - 관행 및 프로세스(Practices and processes) 영역는 SBOM을 업데이트하고 제공해야 하는 방법과 시기와 관련된 6가지 요구사항[7]을 정의

(SBOM 활용) SW 공급망 참여자들은 SBOM을 통해서 보안취약점, 공개 SW 라이선스 등을 관리할 수 있음

- (알려진 보안취약점 관리) SCA[8] 도구를 이용 SBOM을 생성하고, 이를 기반으로 알려진 보안취약점 정보와 비교하는 방식으로 보안취약점 검출

① SBOM 생성 후 SW 구성요소를 식별하고,'Vulnerabilities' 항목 등에서 알려진 보안취약점 정보(CVE, KEV 등)[9]를 확인

② 상용 및 공개 SW에서 발견된 보안취약점에 대하여 미국 NVD(National Vulnerability Database)가 제공하는 보안취약점 정보 확인(https://nvd.nist.gov/vuln/detail/{CVE_ID})

③ NIST에서 제공하는 보안취약점의 영향범위와 심각도 등을 활용하여 위험 수준을 평가하고 조치 우선순위를 지정[10], CVSS[11]는 NVD 보안취약점 데이터베이스에서 정한 심각도와 기본 점수(Base Score)의 등급으로 위험도를 나타냄(V2.0과 V3.0 두가지 방식으로 제공)

---

7) ① Frequency, ② Depth, ③ Known Unknowns, ④ Distribution and Delivery, ⑤ Access Control, ⑥ Accommodation of Mistake

8) SCA : SW 구성요소 분석(Software Composition Analysis) 기술로 상용 및 공개 SW 도구가 있음

9) CVE(Common Vulnerabilities Exposures)란, 공개적으로 알려진 컴퓨터 보안 결함의 목록, CVE는 보통 CVE ID 번호가 할당된 보안 결함을 뜻함, KEV(Known Exploited Vulnerability)는 악용 사례가 알려진 보안취약점으로써, 공격 가능성이 매우 높아 보완 조치가 시급함

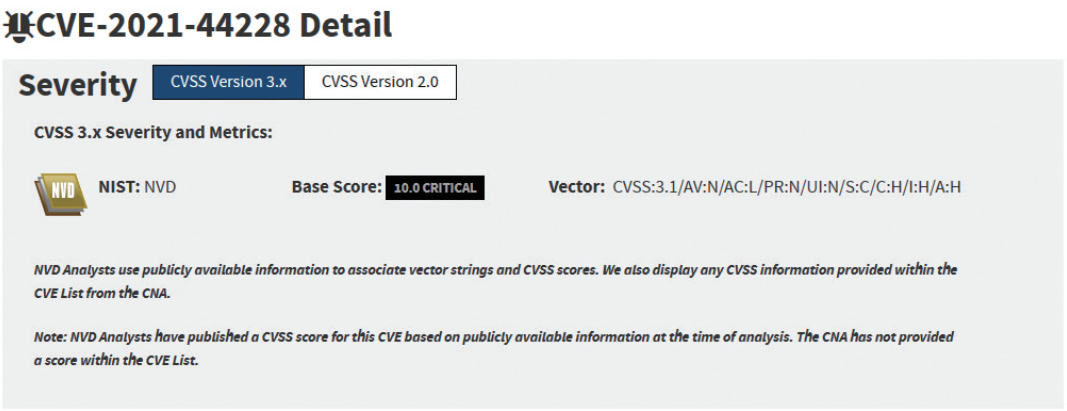
10) https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

11) CVSS(Common Vulnerabilities Scoring System)는 공격자가 보안취약점을 악용할 때 미치는 영향과 보안취약점의 위험도를 나타내며, 0.0 ~ 10.0 숫자가 높을수록 위험도가 더 높음

SBOM에 연계된 보안취약점 정보 예시(CycloneDX 포맷)


```
"vulnerabilities": [
    {
        "bom-ref": "BomRef.6mrtsnb7hug.s911smbt9go",
        "id": "CVE-2019-11405",
        "ratings": [
            {
                "score": 7.4,
                "severity": "high",
                "method": "CVSSv3"
            }
        ],
        "properties": [
            {
                "name": "KEV",
                "value": "false"
            },
            {
                "name": "HEV",
                "value": "true"
            }
        ]
    },
```


NVD를 통한 알려진 보안취약점(CVE) 조회 화면



④ 보안취약점에 대한 조치계획 수립 및 관련자와 보안취약점 정보공유

– 타사 SW 구성요소 등에서 발견된 보안취약점에 대하여 NVD 조치 방안을 확인, 탐지된 보안취약점에 대한 조치계획을 수립하고, 우선순위에 따라 개발기업, 운영기업(기관) 등에 해당 컴포넌트 정보를 공유

– 특히, CVSS 7.0 이상의 높은 위험도를 가진 보안취약점은 보안 담당자 등과 즉각적인 완화조치를 수행하거나, 조치 방안과 시기를 협의할 필요가 있음. 다만, 위험도 판단에는 CVSS 외에 CISA의 KEV 등과 같이 추가적인 지표를 활용할 수 있음

(SBOM의 효과성) SBOM은 SW를 개발하거나, 구매할 때 또는 시스템 운영에도 활용할 수 있음

- **[개발자]**는 공개 SW 및 타사 SW의 구성요소[12]를 사용하여 제품을 만드는 경우가 많음. 이 경우 SW 개발 기업은 SBOM을 통해 해당 구성요소가 최신 버전인지 식별하고, 새로운 취약성에 신속하게 대응할 수 있음
- **[구매자]**는 SBOM을 사용하여 투명하게 취약성 또는 라이선스 분석을 수행할 수 있으며, 이 두 가지 분석은 제품의 전반적인 위험 수준을 평가하는 데 활용할 수 있음
- **[운영자]**는 SBOM을 활용하여 새로 발견된 보안취약점이 잠재적 위험에 노출되어 있는지를 쉽고 빠르게 확인하고 관리할 수 있음

12) SBOM은 기본적으로 SW 구성요소가 가진 종속성(Dependency)을 연결하는 트리(Tree) 구조의 형식으로, 이를 통해 Log4j와 같이 여러 시스템과 패키지에서 사용하는 SW 구성요소를 빠르게 식별할 수 있음

참고 국내외 SBOM 표준화 현황

- SBOM 표준은 SBOM 공유 및 교환을 위한 자동화 요구사항으로 국내에서도 다양한 SBOM 포맷 개발과 표준화가 이루어지고 있음
- 특히, 미국 NTIA에서는 빠른 시장 적용을 위해 3가지(SPDX, CycloneDX, SWID)를 인용, 다만, SWID는 보안취약점 관리에 활용되지 않고 있음

구 분	SPDX	CycloneDX	SWID
목적	라이선스 관리	공급망 보안 관리	미국 정부의 SW 자산 및 보안 관리에 활용
개발 기관	리눅스재단	OWASP	미국 상무부 지원 프로젝트
주요 대상	공개 SW	공개 SW	상용 SW (주로 라이선스 추적·관리)
표준 (년도)	ISO/IEC 5962('21.8월)	–	ISO/IEC 19770-2('15)
파일 형식	.rdf, .xls, .spdx, .json, .yml, .xml	.xml, .json	xml

- 또한, 국내에서도 정부 및 민간 차원에서 각각 SBOM 표준 개발을 위해 노력 중
  - **(민간)** SBOM 단체표준(TTAK.KO-11.0182)은 SPDX v2.0을 참조하여 국내 활용을 위해 개선한 것으로 공개 SW 정보 교환 명세(Open Source Software Package Data Exchange Specification)에 중점을 두었고, 현재는 "공개 SW 공급망 관리를 위한 SW 목록 구성(SBOM) 속성 규격"(TTAK.KO-11.0309, '22.12월)이 있음

  - **(정부)** 국가정보원은 국가·공공기관에 도입되는 SW의 공급망 보안 관리 체계를 구축하기 위해 민관 협력으로 SBOM 기본항목을 개발, NIS-SBOM 기본항목은 ❶ 기본항목 간소화 ❷ 보안취약점 정보연동 ❸ 사이버 위험관리 효율성 향상을 목표로 20개 기본항목을 정의하고 있음

    또한, NIS-SBOM은 20가지 기본항목의 ① SBOM Standard, ② SBOM Type, ③ CycloneDXNo, ④ SPDX Doc. ID, ⑤ SBOM ID, ⑥ Product Name, ⑦ Product Version, ⑧ Component Name, ⑨ Component Alias, ⑩ Component Version, ⑪ Component Supplier Name, ⑫ Component Hash, ⑬ Component Path, ⑭ SBOM Author Name, ⑮ Unique Identifier, ⑯ Dependency Relationship, ⑰ Timestamp, ⑱ License Name Version, ⑲ Vul. DB, ⑳ Vul. Info 임

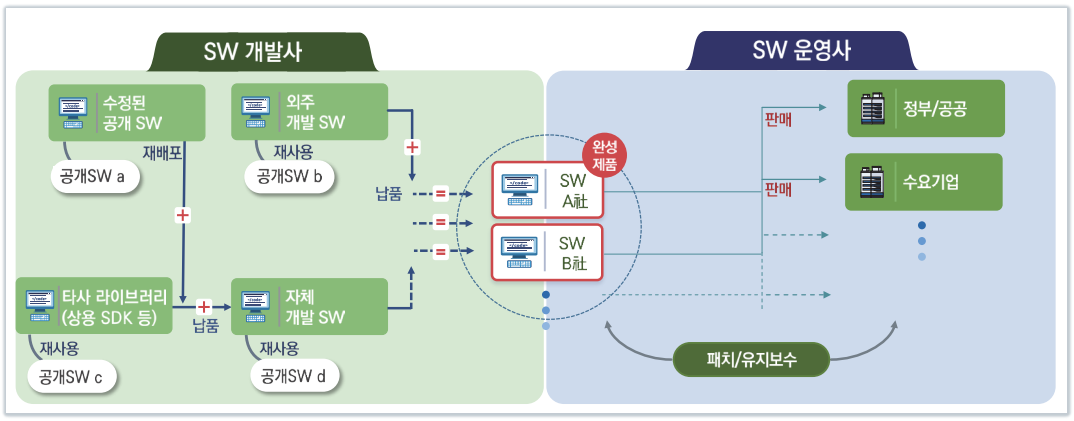
제3장

SBOM 기반 SW 공급망 강화 방안

제1절 SW 공급망 위험관리를 위한 SBOM 확산

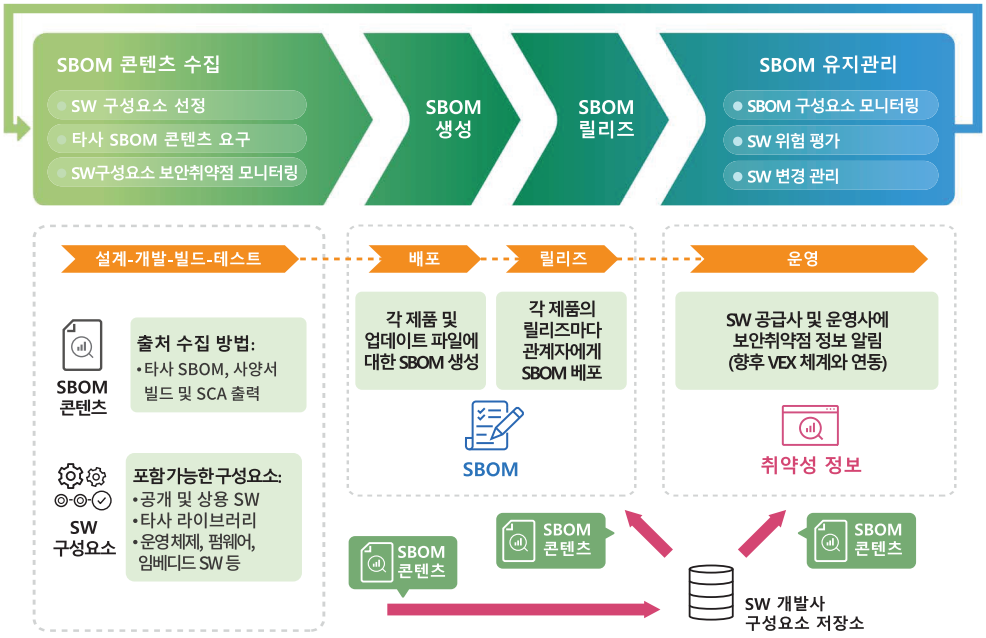
(SBOM 기반 SW 공급망 보안) 외부 SW 또는 자체 개발 SW는 다양한 공개 SW를 포함할 수 있으며, SBOM 기반 SW 공급망 보안 관리 체계를 통해 보안취약점 등 공개 SW 활용에 따른 위험에 대응할 수 있음

내·외부 SW 활용 및 SW 공급망 예시



- 위 그림의 a~d까지 공개 SW가 포함되는 각 SW 개발 생명주기 단계마다 SBOM 관리 체계를 구축하고, 보안 위험이 해소된 SW를 유통해야 함
  - 모든 SW 구성요소에 대한 SBOM 생성이 어려운 경우, 타사 라이브러리 및 공개 SW 구성요소를 중심으로 작성자 등 출처 정보와 종속성 관계(Dependency Relationship)를 관리하는 체계를 우선 구축
- **(개발사)** SW 개발 생명주기 전반에 걸친 SW 위험관리를 위해 기초 데이터가 되는 SBOM 생성을 위한 필수 설비를 구축·활용
  - SBOM 도구(공개 SW 및 상용 도구), SW 구성요소 저장소, SBOM 데이터베이스(DB), SW 위험 평가 및 관리를 위한 자체 보안취약점 DB 및 NVD 연계 등은 SBOM 기반 SW 공급망 보안을 위한 기초 설비임
  - 이와 같은 SBOM 기초 설비를 바탕으로 SW 공급사, 운영사에 대한 SW 구성요소 자산 파악과 보안패치 등을 통해 사이버보안 위협에 선대적 대응 및 신속한 사후 대응도 가능

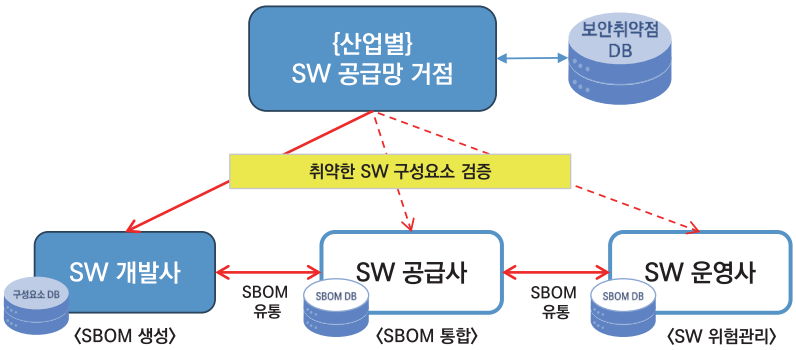
SW 개발 생명주기에 따른 SBOM 관리 체계 구성 방안(개발사)



• **(공급사 및 운영사)** 개발사 → 공급(유통)사 → 운영사로 이어지는 SW 공급망에 대한 SBOM 유통 체계를 구축

– 공공기관 및 협단체 등에 '산업별 SW 공급망 거점'을 구축하고 다수의 공급망 생태계에 검증된 정보를 제공하는 것이 이상적인 체계

산업별 거점을 활용한 SW 공급망 위험관리 구성도



SBOM 기반 SW 공급망 보안 체계의 활용 기대효과

[소비자 신뢰성 향상] 공급망 내 투명한 자산관리, 라이선스 관리, 보안취약점 관리를 통해 소비자들이 안심하고 활용할 수 있는 기반 제공

[글로벌 무역장벽 대비] 미국, 유럽 등 SBOM 제출을 제도화하는 움직임에 체계적으로 대비하여 국가 신뢰도를 높이며, 해외시장 진출을 위한 기업 경쟁력 강화에 도움

제2절 SBOM 기반 SW 공급망 보안 실증

(SBOM 실증) 국내 정부·공공기관 및 민간 기업들의 SBOM 도입 활용과정에서 시행착오를 줄일 수 있도록 ① SBOM 활용 전에 수행하는 SBOM 유효성 분석, ② SBOM을 활용한 컴포넌트 관리사례, ③ SBOM을 활용한 보안취약점 탐지 및 조치 사례를 제시

• **(실증개요)** 국산 SW의 SBOM 생성·활용을 통한 SBOM 기반 SW 공급망 보안 관리 실증

구 분	주요 내용
실증대상	• 의료, 보안 분야 SW 3종(소스코드, 바이너리)
실증도구	• 개발·유통단계 지원 솔루션(1종), 운영·유지보수 단계 지원 솔루션(1종) • 무료 SBOM 생성·점검 지원 도구(2종)
실증내용	• SBOM 생성 및 검증, 보안취약점 탐지·조치, SW 개발기업 대상 공급망 보안 관리 체계 점검 지원

– SW 개발기업의 환경분석을 실시한 후, 담당자 인터뷰를 통해 세부적인 SW 개발환경, 공급망 보안 관리 체계, 대상 SW의 특성 등을 파악

– SBOM을 생성하고 유효성을 검증한 후 검증된 SBOM에서 보안취약점 분석 및 대상 기업의 공급망 보안 관리 체계를 점검

– 이를 기반으로 해당 기업의 SW 개발자 인식 및 개발 프로세스 개선 등 공급망 보안 관리 체계 향상을 위한 보안 컨설팅 제공

• **(SBOM 유효성 검증)** 정확하고 신뢰성이 높은 SBOM을 SW 공급망 내에서 원활하게 유통하고 관리하기 위한 절차

– 자동화된 도구로 SBOM 생성 시, SBOM 항목 일부가 누락 되거나 중복되는 현상 등을 수정하는 절차로 유효성 검증 시 SW 개발자의 참여는 필수

① 개발자의 성향에 따라 의도 또는 비의도적 변경 등으로 일부 SW 구성요소의 누락, 오기 등과 같이 부정확한 SBOM 결과가 생성될 수 있음

* 예시) OPENSSL –〉 OpenSL, SSL 등으로 컴포넌트명을 변경하여 사용

② 소스코드 또는 바이너리 등 대상에 따라 추출한 SBOM 결과가 다르며, 개발언어에 따라 추출한 SBOM 결과도 다를 수 있음(SBOM 도구 도입 시 필수 고려사항)

③ SW 개발과정에서 환경적 요인(개발/구축 시 등)에 따라 개발자가 인지하지 못한 새로운 SW 구성요소가 발견될 수 있음

SBOM 유효성 검증 요령

❶ **(개발자 확인)** 개발자와 함께 SW 제품 개발에 대한 상세 현황 정보와* 추출한 SBOM 데이터를 비교하여 오탐 또는 과탐 여부 등을 검토

* 제품정보 : 기업명, 서비스명, 개발언어, 패키지 형태, 개발 프레임워크, 공개 SW, 상용 SW, 빌드시스템, 형상관리시스템 등

❷ **(완전성 확인)** CycloneDX, SPDX 등 SBOM 표준에서 정한 기본항목 누락 여부 및 항목별 내용이 표준 요구 내용과 일치하는지 확인

• **(SW 컴포넌트 관리)** 개발사들은 공개 SW 또는 제3자 개발 SW의 정확한 컴포넌트 관리를 통해서 SW 자산관리, 라이선스 관리, 보안취약점 관리가 가능

※ 본 실증에서는 ①개발 단계에서는 소스코드, ②유통 단계에서는 바이너리 설치파일을 대상으로 SBOM을 생성하고 분석을 진행

– 대상 SW의 SBOM 분석 결과, 개발자가 인지하지 못한 공개 SW 컴포넌트가 식별되었으며, SW 설치 후 대상 SW와 연결되는 라이브러리에 포함된 공개 SW 컴포넌트도 추가로 발견할 수 있었음

– 또한, SBOM 분석 방식(소스코드 또는 바이너리) 및 사용 도구 종류에 따라 SBOM 정보가 서로 일치하지 않을 수 있음을 확인[13)]

컴포넌트 관리 요령

❶ SW를 개발·유통하는 과정에서 변경·수정되는 SW 제품에 대한 SBOM을 지속 공유해야만, 누락 없는 컴포넌트 관리가 가능

❷ 개발자(기업)가 인지하지 못한 공개 SW 컴포넌트와 SW를 설치 후 생성되는 공개 SW 컴포넌트를 추가하여 관리

❸ 소스코드, 바이너리, 의존성을 종합적으로 분석한 SBOM을 관리하여야, 신뢰성 높은 보안취약점, 라이선스, SW 자산관리가 가능

※ SBOM 유효성 검증 및 SW 컴포넌트 관리는 SBOM 활용의 필수사항으로 요약본에서 소개하였으며, SBOM을 활용한 보안취약점 관리 및 보안 컨설팅 등에 관한 세부사항은 전체본 제3장 참고

13) 분석방식(소스코드와 바이너리)에 따라 SBOM 정보가 상이함, 또한 바이너리 대상 분석은 분석하는 기술과 DB가 달라서 도구 간 격차가 큰 것으로 판단, 신뢰성 높은 SBOM 생성 및 유통을 위해 2개 이상의 도구를 이용한 교차 검증이 필요

제3절 SW 보안취약점 점검 지원 테스트베드

(기업지원허브, 판교) 일반 국민들과 중소기업들의 애로사항을 해결하기 위하여 기업지원허브를 개소하고, 사이버보안 위협 시연 및 보안취약점 점검, 견학·교육 프로그램 등을 지원('15.10월~)

- **(사이버보안 위협시연)** 디지털기술의 융·복합 확산 동향에 맞춰서 연차별로 분야를 확대 및 개선하여 서비스 중[14)]
- **(보안취약점 점검지원)** 다양한 디지털 제품·서비스의 보안 내재화를 위해 중소기업 등이 자체 검증하고 보완할 수 있는 환경 제공
  - SBOM 도구(소스코드, 바이너리) 등 전문 도구를 활용하여 다양한 분야의 디지털제품 및 서비스의 소스코드, 펌웨어, 통신 프로토콜 등의 보안취약점 점검 지원

(디지털헬스케어 보안 리빙랩, 원주) 디지털헬스케어기기 등에서 발생할 수 있는 사이버보안 위협 시연, 디지털헬스케어 기기 및 서비스에 대한 보안성 테스트 등 기업 지원을 위해 구축('20.12월)

- **(사이버보안 위협시연)** 다양한 분야의 종사자들이 디지털헬스케어 기기 및 서비스에 대한 사이버위협을 체감할 수 있도록 ① 환자 의료정보 모니터링 시스템 데이터 변조, ② 영상정보처리시스템 데이터 변조, ③ 개인의료장비(심박기, 약물주입기) 트래픽 변조를 통한 오작동 유도, ④ 네트워크(통신 구간 미암호화) 보안취약점을 통한 병원 모니터링을 다양한 시나리오를 통한 위협 시연
- **(보안취약점 점검지원)** 디지털헬스케어기기의 네트워크 보안취약점 점검, 소스코드 보안취약점 점검 등을 지원 중, '24년 상반기부터 SBOM 생성 도구를 도입하여 SBOM 생성 및 보안취약점 조치를 지원
- **(의료기기 인허가 지원)** 디지털헬스케어 보안리빙랩에서 보안취약점 조치 확인서를 받아서 의료기기 인·허가시 첨부할 경우 사이버보안 시험항목은 기준을 만족한 것으로 갈음
  - 디지털헬스케어기기 인허가 지원은 식약처와 협의를 통해 연 8~9건을 선정하여 지원

(국가사이버안보협력센터 기술공유실, 판교) 급격하게 발전하는 ICT 기술의 안전성을 선제적으로 확인하고, 보안업체·시험기관에게 고가·신기술 융합제품에 대한 안전성 평가 기술 지원('22.11월 개소)

- **(공급망 보안 테스트베드)** Log4j·3CX 등 공개 SW의 보안취약점을 악용한 공급망 공격이 지속 발생함에 따라 SW 공급망 보안 강화를 위해 ❶ SBOM 생성 자동화 ❷ SBOM 관리 ❸ SW 보안취약점 추적·관리 등을 실증할 수 있는 테스트베드의 필요성 대두
  - 국가·공공기관에 도입되는 SW제품의 투명성 및 신뢰성을 확인하고 보안취약점을 식별·추적할 수 있는 SBOM 기반 공급망 보안 관리 체계를 실증할 수 있는 테스트베드를 기술공유실에 구축
  - 국내외 상용 SW 분석도구(SCA) 3종이 선별 적용되었으며, 분석도구를 활용 SBOM 생성 및 유효성 검증을 실시

14) 홈 · 에너지('15), 교통('16), 의료('17), 안전 · 재난 · 환경('18), 건설('19) 분야 시연환경, 홈 리빙랩('20) 구축, 테스트베드 VR('21), 메타버스('22) 제작 및 드론 · 의료 시연환경 개선('23) 등 현재 6종의 사이버보안 위협 시연

– 신뢰성 높은 SBOM 생성도구의 조건 네 가지를 식별할 수 있었으며, 각 도구의 장점을 통합한 SBOM 통합엔진을 개발, 테스트베드에 적용

• **(발전계획)** 향후 산·학·연 전문가들과 SW 공급망 보안 통합관리 체계 구축 방안을 지속적으로 논의하면서 각 방안들을 실증할 수 있는 테스트베드로 발전시켜 나갈 계획

제4절 SBOM 기반 SW 공급망 보안 발전 제언

가. 개발기업의 SW 투명성 확보 지원

국내 중소기업들이 SW 공급망 보안 체계를 구축하기 위해서는 인력 및 시설 등에 대한 투자가 필요하며, 기업들의 이와 같은 초기 투자에 대한 부담을 완화하기 위해서 범정부 차원의 지원센터 운영, SBOM 기반의 SW 공급망 보안 관리 체계 도입 지원 및 SW 공급망 보안 관리 공통모델 연구 필요

나. SBOM 및 SW 공급망 보안에 대한 적극적 투자

기업 차원에서 SW 공급망에 대한 사이버 위협에 대응하고, 미국 및 유럽 등 주요국 시장에서 추진하고 있는 무역장벽에 대응하기 위해 SBOM 및 공급망 보안 기술 확보를 위한 적극적인 투자가 필요. 보안 수준이 높은 기업은 신뢰도가 향상되고, 신뢰도가 높은 기업의 제품 및 서비스는 소비자가 믿고 구매할 수 있음을 잊지 말아야 할 것임

다. 공급자와 수요자가 연계되는 SBOM 기반 공급망 보안 관리

기관 내 IT 자산과 SW, 그리고 SW의 구성요소를 같이 관리하고 관련 보안취약점을 지속적으로 모니터링할 수 있는 입체적인 관리 체계를 구축할 필요. 이렇게 함으로써 SW 개발기업과 수요기업의 공급망 관리 체계가 연동될 수 있다면 상호 시너지 효과를 발휘할 수 있고, 산업 전반에서 선순환 효과를 창출할 수 있게 될 것임

라. 안전한 SW 개발 환경 조성 등 사이버 복원력 강화

SW 위험관리 및 사이버 복원력을 강조하고, 향후 이를 제도적으로 구체화하고 실행하기 위한 법적, 기술적 프레임워크를 도입할 필요. 시장에 공급되는 SW 제품 및 서비스 등의 생애주기 전반에서 보안관리를 강화하고, 소비자가 보안성 내재화 여부를 고려할 수 있도록 제도화(보안적합성, IoT 보안 라벨링 등) 하는 방안도 필요

마. SBOM의 안전한 활용 및 기밀성 보장 기반 공유 방안

SBOM은 기업들이 공개를 꺼리는 다양한 정보를 포함할 수 있음. 따라서 SBOM 활용에 따른 SW 개발기업의 리스크를 최소화하면서도 보안취약점 관리를 통해 수요자의 보안 리스크도 동시에 최소화 할 수 있는 방안 필요. 이를 해결하기 위해 SBOM의 기밀성을 보장하면서 동시에 SBOM을 안전하게 공유하는 기술에 대한 다양한 연구가 필요

과학기술정보통신부

국가정보원

대통령직속
디지털플랫폼정부위원회

요약본 **SW 공급망 보안 가이드라인** v 1.0

2024년 5월 13일 1판 1쇄

발행처 한국인터넷진흥원
나주시 진흥길 9 한국인터넷진흥원

제 작 국가정보원, 과학기술정보통신부, 디지털플랫폼정부위원회,
한국인터넷진흥원

SW 공급망 보안 가이드라인 v 1.0

SW 공급망 보안 국제동향 및
SBOM 활용사례

요약본