과학기술정보통신부 | 대통령직속 디지털플랫폼정부위원회 | 보도자료 | 다시 대한민국! 새로운 국민의 나라

보도시점 2024. 5. 12.(일) 12:00 (2024. 5. 13.(월) 조간) 배포 2024. 5. 10.(금) 14:00

정부, 소프트웨어 공급망 보안 지침(가이드라인) 1.0 발표

(부제 : 소프트웨어 공급망 보안 국제동향 및 소프트웨어 구성명세서(SBOM) 활용사례)

- 국산 소프트웨어에 소프트웨어 구성명세서(SBOM) 실증결과를 반영한 지침(가이드라인) 마련 -

- 디지털플랫폼정부 시스템 등에 소프트웨어 공급망 보안을 시범적용하고, 중소기업 소프트웨어 공급망 보안 역량 강화 지원 확대 -

- 해외동향과 국내 준비상황을 면밀히 살피면서 제도화 준비 -

과학기술정보통신부(장관 이종호, 이하 '과기정통부'), **국가정보원**(원장 조태용, 이하 '국정원'), **디지털플랫폼정부위원회**(위원장 고진, 이하 '디플정위')는 민관 협력을 통해 **'SW 공급망 보안 가이드라인 1.0 (이하 '가이드라인')'**을 마련했다고 밝혔다.

> 가이드라인은 **과기정통부**, **국정원**, **디플정위**와 **한국인터넷진흥원**(KISA), **정보통신산업진흥원**(NIPA), **한국정보보호산업협회**(KISIA) 등 **정부·공공기관 홈페이지**를 통해 **2024년 5월 13일(월) 12:00**부터 **무료로 내려받아 사용할 수 있음**

본 가이드라인은 확산되고 있는 **SW 공급망 사이버보안 위험**과 미국, 유럽 등 해외 **주요국의 SW 구성요소 명세서**(SW Bill of Materials, SBOM) **제출 의무화 등에 대응**하여 **정부·공공 기관 및 기업**들이 자체적인 **SW 공급망 보안 관리역량을 갖출 수 있도록** 지원하기 위해 마련되었다.

또한 본 가이드라인은 **국산 SW에 대한 SBOM 실증** 및 **SW 공급망 보안 테스트베드**(판교) **시범 운영 결과** 등을 반영한 것으로 **세계적으로도 유례없는 실무 안내서**이며, 향후 **미국 등 주요 국가와 협력**을 통해 **해외에도 적극 소개**할 계획이다.

가이드라인은 전체본(100여 페이지)과 **요약본**(16 페이지)으로 제공되며, **정부·공공기관의 정책결정자** 및 **기업의 경영진** 등은 **요약본**을 통해서 **쉽고 빠르게 SW 공급망 보안**에 관한 **주요 내용을 이해**할 수 있을 것으로 기대된다.

국내 중소기업들에게 **SW 공급망 보안**은 **전문인력과 SBOM 생성 도구 등 전용 시설**을 갖춰야 하는 **현실적인 어려움으로 초기 투자에 상당한 부담**이 될 수밖에 없으나 **피할 수 없는 숙제**와 같은 것이다.

이와 같은 **기업들의 애로사항을 해결**하기 위해 정부는 **기업지원허브**(판교), **디지털헬스케어 보안리빙랩**(원주), **국가사이버안보협력센터 기술공유실**(판교) 등에 **SBOM 기반 SW 공급망 보안 관리체계**를 구축하고 **기업 지원 서비스**를 제공하고 있다.

특히, 가이드라인에는 **정부·공공 기관 및 기업**들이 **SBOM 기반 SW 공급망 보안 관리체계**를 도입하는 과정에서 **시행착오를 줄일 수 있도록 SBOM 유효성 검증, SW 구성요소 관리 요령 및 SBOM 기반 SW 공급망 보안 관리 방안** 등을 상세하게 수록하였다.

정부는 이 가이드라인이 **다양한 산업분야**에서 **활용될 수 있도록 홍보**하는 한편, **디지털플랫폼정부 주요시스템 구축** 시 **SBOM을 시범 적용**하여 **우수 사례를 도출하여 발전시켜 나갈 계획이다.**

SBOM 도입 등의 제도화는 필요하지만, **체계적인 준비 없이 제도를 성급하게 도입**할 경우 **SW 개발기간이 장기화되고, 원가 상승요인으로 작용**하여 **기업들의 부담 요인이 될 수** 있다.

따라서 **정부는 기업들에 대한 SBOM 적용 지원을 강화하면서 SW 공급망 보안 저변을 확대하고, 향후 주요국의 제도화 동향과 국내 산업 성숙도를 고려하며 점진적으로 제도화를 준비해나갈 방침이다.**

또한, **올해 하반기**에는 **산·학·연 전문가**들이 참여하는 **범정부 합동TF**를 구성하여 **세부적인 정부지원 방안, 제도화 추진방향** 등에 대한 **심도 있는 논의**를 진행한 후 **'SW 공급망 보안 로드맵'**을 마련할 계획이다.

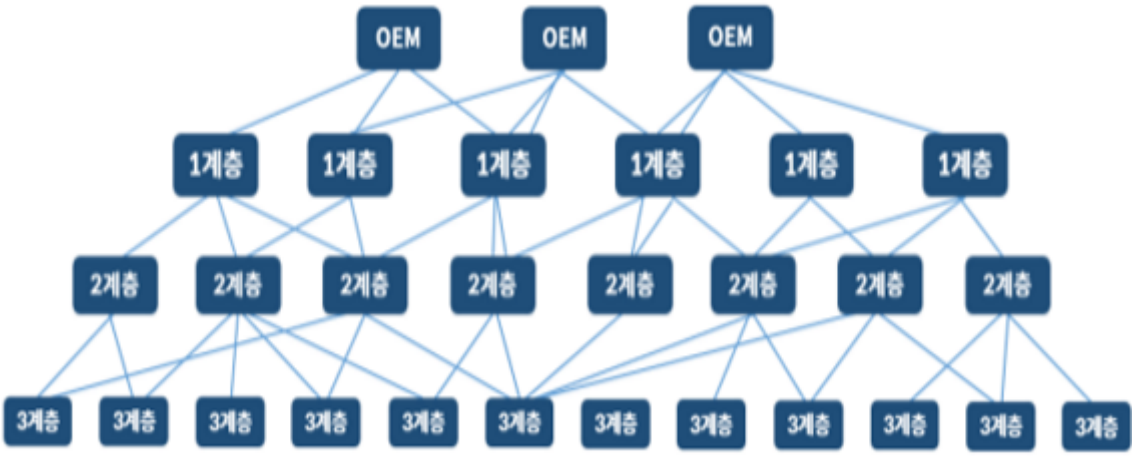
과기정통부	정보보호산업과	책임자	과 장	정은수 (044-202-6450)
		담당자	사무관	김성환 (044-202-6451)
국정원				(111)
디플정위	안전활용지원과	책임자	과 장	최충호 (02-750-4760)
		담당자	사무관	정홍순 (02-750-4756)
KISA	디지털안전본부	책임자	팀 장	이향진 (061-820-1283)
		담당자	책임연구원	김성훈 (061-820-1882)
KISIA	산업지원단	책임자	단 장	황지은 (02-6748-2004)
		담당자	팀 장	정호준 (02-6748-2006)

붙임 SW 공급망 보안 가이드라인 1.0 주요내용

□ 제1장 추진배경

(환경변화) SW 개발-공급(유통)-운영의 연결성(Connectivity)으로 인해 생태계 참여 계층의 범위가 점점 확장되고 있다. 모바일, 사물인터넷(IoT), 클라우드 등 디지털 제품 및 서비스 개발, 공급(유통)에서 외부 SW의 활용이 늘어나고 있으며, 다양한 정보통신기술(ICT)과의 상호 의존성(Dependency)도 증가하고 있다. 공개 SW인 Log4j의 보안취약점을 악용한 사이버 공격(2021년)은 웹 방화벽 등 다양한 방법으로 방어할 수 있지만 이보다 더 큰 위험은 Log4j가 어느 제품 또는 서비스에 어떻게 사용되고 있지는 정확히 파악하기 어렵다는 데 있다.

< 최종자 생산자(OEM)를 중심으로 공급망 생태계 기본 모형 >



(주요국 정책동향) 미국은 2021년 5월 행정명령(EO 14028)을 통해 연방정부에 납품되는 SW의 SBOM 제출을 발표한 이후 올해 3월 이를 보완하는 보안관리 자체증명서(Self Attestation Form)를 확정하고, 본격 시행을 앞두고 있다. 유럽 또한 역내에 유통되는 디지털 제품 및 서비스의 보안 강화를 위해 '사이버 복원력법(Cyber Resilience Act)' 을 제정 발의하고(´22.9월), 작년 12월 제정법안에 대해 EU 집행위원회(Commission), EU 의회(Parliament), EU 이사회(Council) 간 정치적으로 합의를 완료하였고, 올해 승인 절차를 거쳐 2026년 이후 시행될 전망이다.

□ 제2장 SW 공급망 위험관리 방안

(공급망 참여자의 역할) 공급망 사이버보안 위험은 공급자, 공급망, 제품 및 서비스에서 발생할 수 있는 피해 가능성으로 정의할 수 있으며, 개발사, 공급(유통)사, 운영사가 각자의 역할을 완수해야 SW 공급망 전체의 보안 위협을 관리할 수 있다.

[개발사] SW의 설계, 구현, 검증 등 개발단계에서 보안 활동을 통해 보안취약점을 최소화해야 할 뿐만 아니라, SW에 포함된 라이브러리와 빌드 및 배포 체계의 보안성을 확보

[공급사] 보안 요구사항 충족 여부 확인, 타사 SW의 검증, 실행 파일 테스트를 통해 SW 제품의 보안을 검증하고, 취약점을 발견했을 때는 고객(운영)사에 이를 알리고, 취약점에 대응

[운영사] 보안 요구사항과 공급망 위험관리(SCRM) 요구사항을 정의하고, 그에 따라 SW 인수테스트를 진행하며, 제품 적용 및 생명주기 관리에 필요한 보안 및 공급망 위험관리 대책을 이행

(SBOM 활용) SW 개발 시에 공개 SW 등 외부 SW를 포함하여 개발하고 있어서 이에 따라 SW 공급망이 복잡해지고, 악성코드 및 보안취약점 관리에 대한 필요성이 대두되었으며, SW 개발-공급(유통)-운영 등 공급망 각 단계에서 SBOM을 활용함으로써 SW 구성요소를 안전하게 관리할 수 있으며, SBOM을 활용하여 SW 자산관리, 공개 SW 라이선스 및 보안취약점 관리가 가능하다. 개발사 및 운영사적 측면에서 SBOM 활용의 장점은 아래와 같다.

[개발사] 공개 SW 및 타사 SW의 구성요소를 사용하여 제품을 만드는 경우가 많음. 이 경우 SW 개발 기업은 SBOM을 통해 해당 구성요소가 최신 버전인지 식별하고, 새로운 보안취약점에 신속하게 대응할 수 있음

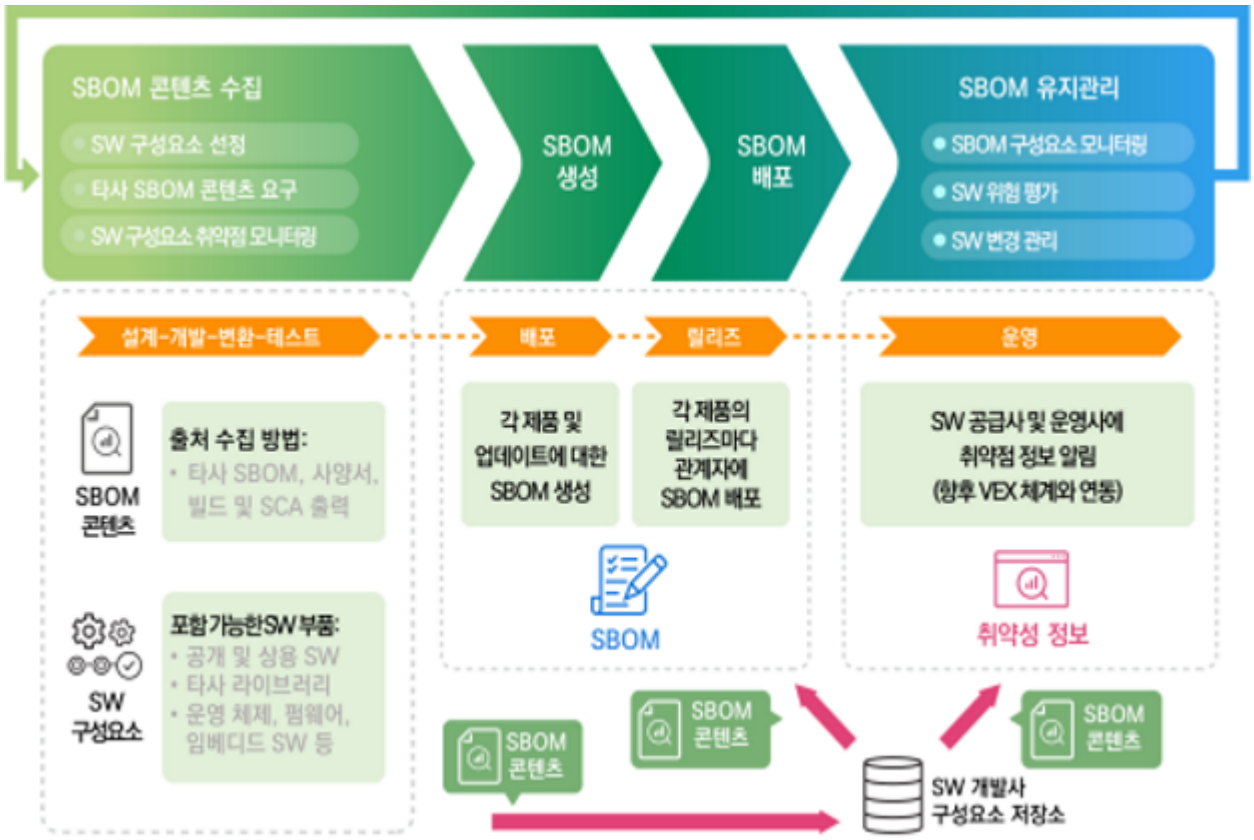
[운영사] SBOM을 활용하여 새로 발견된 보안취약점이 잠재적 위험에 노출되어 있는지를 쉽고 빠르게 확인하고 관리할 수 있음

< SBOM 활용의 효과성 >

(SBOM 기반 SW 공급망 보안) 외부 SW 또는 자체 개발 SW는 다양한 공개 SW를 포함할 수 있으며, SW 개발 생명주기 단계마다 SBOM 생성 및 배포 체계를 구축하고, 보안 위험이 해소된 SW를 공급(유통)함으로써 SW 공급망의 투명성과 신뢰성을 확보할 수 있다.

SW 개발 생명주기 전반에 걸친 SW 위험관리를 위해 기초 데이터가 되는 SBOM 생성을 위한 필수설비 구축이 필요하며, SBOM 도구(공개 SW 및 상용 도구 활용), SW 구성요소 저장소, SBOM 데이터베이스(DB), SW 위험 평가 및 관리를 위한 자체 보안취약점 DB 등 SBOM 기반의 SW 공급망 보안 기초 설비 확보가 필요하다.

< SW 개발 생명주기에 따른 SBOM 구성 방안 >



□ 제3장 SBOM 기반 SW 공급망 보안 실증사례

(실증개요) 국산 SW의 SBOM 생성·활용을 통한 SBOM 기반 SW 공급망 보안 관리 실증을 위해 실증계획을 수립하였으며, 이에 따라 SW 개발기업의 환경 분석을 실시한 후, 담당자 인터뷰를 통해 세부적인 SW 개발환경, 공급망 보안 관리 체계, 대상 SW의 특성 등을 파악하였다.

SBOM을 생성하고 유효성을 검증한 후 검증된 SBOM에서 보안취약점 분석 및 대상 기업의 공급망 보안 관리체계를 점검하였고, 이를 기반으로 SW 개발자 인식 및 개발 프로세스 개선 등은 물론 향후 공급망 보안 관리체계 향상을 위해 보안 컨설팅도 제공하였다.

< 국산 SW SBOM 실증 개요 >

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 관리체계 점검 지원

(SBOM 유효성 검증) 신뢰성이 높은 SBOM을 SW **공급망 내에서 원활하게 유통**하고 관리하기 위한 것이며, **자동화된 SBOM 도구**로 SBOM 생성 시, SBOM 항목 **일부가 누락 되거나 중복되는 현상** 등을 제거하는 절차로 SW 개발자 참여는 반드시 필요하다.

< SBOM 유효성 검증 요령>

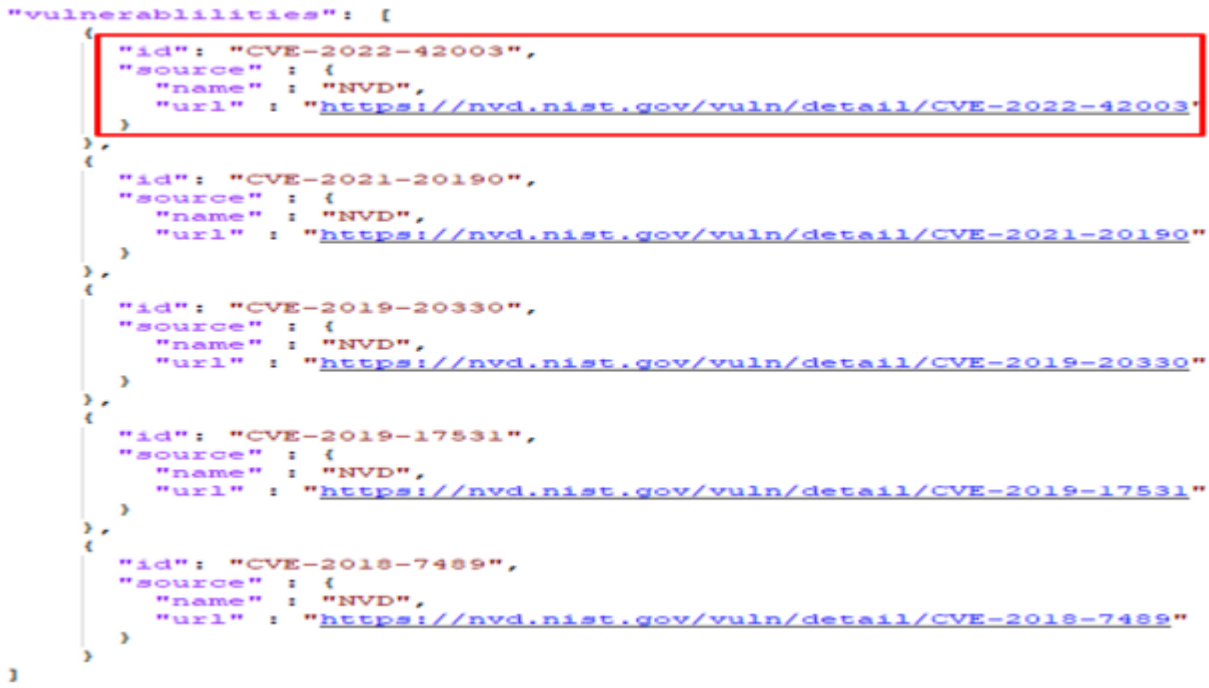
❶ **(개발자 확인) 개발자와 함께 SW 제품 개발에 대한 상세 현황 정보와 추출한 SBOM 데이터를 비교하여 오탐 또는 과탐 여부 등을 검토**

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

(보안취약점 관리) SW의 보안취약점 탐지 및 조치를 위해서는 SBOM 생성을 통한 SW 구성요소 관리가 필요하다. 또한 대상 SW의 유형(소스코드 또는 바이너리)에 따라 생성된 SBOM의 구성요소 명세가 다를 수 있고, 그에 따라 보안취약점 탐지 결과도 상이할 수 있으므로 SBOM 유효성 검증을 통해 SBOM의 신뢰성을 높이는 것이 효과적인 보안취약점 관리를 필수요건이 될 수 있다.

실증 기업 A의 SW 소스코드와 바이너리를 대상으로 SBOM을 생성하고, 이를 취약점 DB와 비교하여 보안취약점을 검출하였다. 그림과 같이 CycloneDX 표준을 이용하는 SBOM에서는 'Vulnerabilities' 항목에서 취약점 정보 확인이 가능하다.

< SBOM을 활용한 보안취약점 탐지(예시)



발견된 보안취약점에 대한 더 자세한 정보 및 조치 수단은 미국 NIST의 보안취약점 데이터베이스(NVD, https://nvd.nist.gov/vuln/detail/(CVE 코드명))에서 확인할 수 있다. SBOM 도구에 따라 CVE-ID, 취약점 출처(취약점 소스명, URL), 조치방안 등 보안취약점의 상세 항목이 다르게 표현될 수 있으므로 지속적인 활용을 통해 경험을 축적할 필요가 있다.

< SBOM 기반 SW 공급망 보안 관리 요령>

❶ **대상 SW 개발언어의 호환성, 도구의 분석 알고리즘, 기업의 공급망 특성 등을 꼼꼼하게 확인하여 SBOM의 신뢰성을 높일 수 있는 적합한 SBOM 도구 선정**

❷ **소스코드 또는 바이너리 분석방식 선택은 기업의 환경에 맞게 하되, 2개 이상의 도구를 상호 보완적으로 활용하는 것을 권장(상용 SBOM 도구 외에도 무료 도구 선택 可)**

❸ **설계-개발-공급(유통)-도입 및 운영-유지보수 등 공급망 각 단계별로 SBOM을 생성·공급(유통)할 수 있는 관리체계를 구축할 것을 권고**

❹ **보안취약점 탐지 성능을 높이기 위해 SBOM DB 구축, NVD(NIST의 보안취약점 데이터베이스) 등과 연동 체계구축 필요**

❺ **보안취약점 탐지 시, 신속하게 개발자(부서, 기업 등)에 전파하여 조치계획을 수립하고, 고객(운영)사에도 적의 조치할 수 있는 체계 구축 필요**

□ 제4장 SBOM 기반 SW 공급망 보안 활성화 지원

우리나라는 SW 공급망 사이버보안 위험 증가와 미국, 유럽 등 주요국의 SBOM 제도화에 대응하여 국내 중소기업들의 자체적인 SW 공급망 보안 역량 강화를 중점 지원하고 있다. 기존 기업지원 시설에 SBOM 도구를 확충함으로써 SW 기획, 개발단계에서부터 SW 악성코드 및 보안취약점이 관리될 수 있도록 지원하고 있다.

(기업지원허브, 판교) 일반 국민들의 사이버위협에 대한 막연한 걱정을 해소하고, SW 기획·개발단계부터 보안이 내재될 수 있도록 지원하기 위하여 기업지원허브를 개소하고, 사이버보안 위협 시연 및 보안취약점 점검, 견학·교육 프로그램 등을 운영(´15.10월~)하고 있다.

(디지털헬스케어 보안 리빙랩, 원주) 디지털헬스 기기 등에서 발생할 수 있는 사이버보안 위협 시연, 디지털헬스케어 기기 및 서비스에 대한 보안성 테스트 시설을 구축하고, 디지털헬스케어 제품 및 서비스에 대한 보안취약점 점검을 지원(´20.12월~)하고 있다.

(국가사이버안보협력센터 기술공유실, 판교) 급격하게 발전하는 ICT 기술의 안전성을 선제적으로 확인하고, 보안업체·시험기관에게 신기술 융합제품에 대한 안전성 평가 기술 지원을 위해 개소(´22.11월) 하였으며, Log4j·3CX 등 공개 SW의 보안취약점을 악용한 공급망 공격이 지속적으로 발생함에 따라 SW 공급망 보안 강화를 위해 ❶ SBOM 생성 자동화, ❷ SBOM 관리, ❸ SW 보안취약점 추적·관리 등을 실증할 수 있는 시설을 갖추고 시범운영 중이다. 향후 산·학·연 전문가들과 SW 공급망 보안 통합관리 체계를 구축 방안을 지속적으로 논의하면서 각 방안들을 실증할 수 있는 테스트베드로 발전시켜 나갈 계획이다. 끝.