SCSC: 상호참조 기반 공급망 보안 관리체계 및 통합 플랫폼 제안

최하경, 유예서, 장인영, 이혜인

덕성여자대학교 (학부생)

Supply Chain Security Cross-reference Framework and Platform Proposal

HaKyeong Choi, Yeseo You, Inyeong Jang, Hyein Lee

Duksung Women's University (Undergraduate Students)

요 약

현재 수출입 안전관리제도(AEO), 정보보호 관리체계 인증(ISMS-P), 소프트웨어 공급망 보안(SBOM) 제도는 각각 독립적으로 운영되고 있어, 기업이 유사한 보안 항목에 대해 중복 심사를 받는 비효율이 발생하고 있다. 또한 AEO 제도는 물리적 보안 중심의 평가에 머물러, EOL/EOS(지원 종료 소프트웨어)와 같은 기술적 사이버 위협에 대한 대응이 제한적이다. 본 연구에서는 이러한 문제를 해결하기 위해 세 제도를 연계한 공급망 보안 통합 플랫폼 구축 방안을 제안한다. 제안 모델은 (1) AEO와 ISMS-P의 공통 심사 기준을 표준화하여 상호 참조가 가능한 인증 체계를 마련하고, (2) SBOM 데이터를 활용해 EOL/EOS 사용 여부를 자동 검증함으로써 기술적 보안 심사의 실효성을 강화하며, (3) 기업의 민감한 원본 서류를 이동시키지 않는 'Zero-Copy' 기반의 메타데이터 공유 플랫폼을 통해 기관 간 안전한 정보 연계를 구현한다. 이를 통해 기업은 중복 규제 대응 부담을 완화하고, 국가는 공급망 전반의 사이버 보안 수준과 산업 경쟁력을 향상시킬 수 있을 것으로 기대된다.

Ⅰ. 서론

오늘날의 소프트웨어 공급망은 다수의 오픈소스·서드파티 라이브러리로 구성되어, 랜섬웨어·APT 등 고도화된 공격에 지속적으로 노출되어 있다[1]. 특히, 단일 소프트웨어 컴포넌트의 취약점이나 EOL/EOS의 사용은 생태계 전반으로 빠르게 전파되어 심각한 서비스 중단과 공급망 피해를 유발할 수 있다. 그러나 ISMS·AEO와 같은 현행 인증 제도는 관리·절차적 통제에 치중하여, 개별 소프트웨어 구성요소 수준의 기술적 위험을 식별하고 통제하는 데에 명백한 한계를 보인다.

본 연구는 이 한계를 극복하기 위해 SBOM 기반의 기술적 검증 데이터를 ISMS·AEO 인증 프로세스와 연계하는 통합 보안 관리 모델을 제안한다. 이를 통해 소프트웨어 구성요소 단위의 가시성과 예방적 취약점 관리를 확보하고, 공급망 전체의 보안 신뢰도를 향상시키는 것을 목표로 한다.

Ⅱ. 정책 현황 및 문제점

국내 보안 관리 체계는 AEO, ISMS/ISMS-P, SBOM 가이드라인 등 여러 제도가 운영되고 있으나, 제도 간 연계성이 부족하고 SBOM의 법제화가 이루어지지 않아 통합적인 대응에는 한계를 보인다.

관세청이 주관하는 AEO 인증은 법규 준수, 내부통제 등을 주로 평가하며 사이버 보안은 권고 수준의 선택적 항목으로 다룬다[2]. 반면, ISMS-P 인증은 과학기술정보통신부·KISA·개인정보보호위원회가 관장하는 법정 제도로, 접근통제나 EOL/EOS 관리 등 구체적인 기술적·관리적 보호조치를 명시하고 있다[3]. 최근 발표된 '소프트웨어 공급망 보안 가이드라인'은 SBOM 기반의 관리 체계를 제시하였으나, 법적 구속력이 없는 권고안의 성격을 갖는다[4].

이처럼 각 제도는 접근통제, 취약점 관리 등 일부 공통된 보안 통제 요소를 포함함에도, 소관 부처와 법적 근거의 차이로 인해 단절적으

로 운영되고 있다. 이로 인해 기업은 유사 항목에 대한 중복 인증 부담을 겪게 되며, 정부는 EOL/EOS 관리 기준의 불일치나 사이버 보안 평가의 공백으로 인해 공급망 전반의 위험을 통합적으로 관리·감독하는 데 어려움을 겪는다. 이러한 비효율과 정책적 공백은 국가 전체의 공급망 보안 대응 역량을 저해하는 핵심 요인으로 작용한다.

Ⅲ. 정책 제안 및 시행 전략

1. 정책 제안

AEO-ISMS-SBOM의 공통 통제를 '공통 심사 기준 부속서'로 제정하고, 각 제도 문서에 상호 참조 및 교차인정 조항을 신설하여 1회 제출만으로 다수의 제도에서 재사용할 수 있도록 한다. 이를 지원하기 위한 수단으로 원문을 이동하지 않고 메타데이터만 공유하는 Zero-Copy 기반 '공급망 보안 통합 플랫폼'을 신설·운영한다. 모든 제도는 각 기관의 법·표준에 부합하도록 설계한다.

2. 정책 구성 요소

1) 공통 심사 기준 부속서 신설

AEO·ISMS-P·SBOM 간 공통 통제 5개 축(접근통제, 로그·감사, 외부자·거래처, 운영 보안[취약점·패치], 자산/구성[SBOM])을 코드 단위로 1:1 대응시킨다. 우선적으로 AEO 인증 대상 기업과 ISMS-P 의무 조직에 적용한다. 각 항목별 허용 증빙과(정책문서, 절차서, 로그기록, 취약점 보고서, SBOM 등) 유효기간을 표로 명시하며, 상호참조의 적용 수준을 단계별로 정의하고, 항목별 허용 단계를 부속서에 명시한다.
재사용 가능한 증빙으로는 각 영역별로 분류할 수 있다. 우선 접근통제 영역에서는 계정 목록, 권한표, 접속 로그가 재사용 가능한 증빙이 된다. 이를 통해 계정·권한·접근기록 관리와 배포 권한 정책 준수 여부를 입증할 수 있다.
로그·감사 영역에서는 접속·변경 로그 보존 내역, 로그 관리 체계, SIEM 리포트와 보존 정책이 증빙 자료로 활용될 수 있다. 빌드 메타데이터와 타임스탬프 역시 무결성 검증과 재현성 확인을 위한 증빙이 된다.
외부자·거래처 보안 검증 측면에서는 협력업체 보안 평가 체크리스트, 계약서, 그리고 제3자 컴포넌트 출처를 명시한 SBOM(SPDX)이 재사용 가능한 증빙이다. 취약점·패치 관리 분야에서는 CVE 매칭 리포트, 패치 내역 기록, SBOM, 취약점 리포트가 주요 증빙으로 활용될 수 있다. 마지막으로, 자산·구성 관리 측면에서는 자산대장, 시스템 목록, 정보자산 식별 내역, SBOM 파일이 재사용 가능한 증빙으로 인정될 수 있다.

2) 상호 참조(교차 인정) 조항 신설

부속서에 따라 범위, 유효기간, 증빙의 유형을 지정하고 타 제도의 성과를 간소화 및 대체로 인정한다. 또한 AEO에서의 EOL/EOS 관련 조항을 신설하여 물리적 공급망 보안을 강화시킨다. 신설 조항의 예시는 다음 표와 같다.

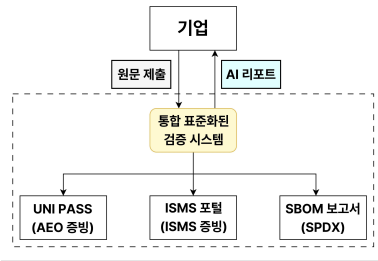
구분	신설·개정 조항	예시(안)
AEO 고시 (관세청)	제○조 (상호참조)	관세청장은 ISMS-P 인증 결과 중, 공통 심사 기준에 해당하는 항목을 AEO 심사 시에 간소화할 수 있다. 간소화 범위와 유효기간은 부속서 ○호에 따른다.
	제○조 (소프트웨어 EOL/EOS 관리)	1. 관세청장은 공인 신청인 및 기업에 대하여, EOL/EOS 자산의 식별·평가·대응 계획 수립 여부를 사이버 보안 하위항목으로 심사할 수 있다. 2. EOL/EOS로 판정된 자산에 대해서는 업그레이드·교체·격리 등의 대응 계획과 예상 기한을 제시하여야 한다.
ISMS-P (KISA)	운영보안 항목 개정	운영보안(취약점/패치)에 대한 증빙은 SPDX형식의 SBOM 및 취약점 매칭 보고서로 대체 가능하다.
공통 조항 (사후관리)	상호참조 유효기간 12개월	상호참조에 대한 인정은 최대 12개월 유효하며, 만료 시에 재검토된다. 경과 기간동안 기존 절차와 병행 가능하다.

[표 2] 신설 조항 예시(안)

3) 공급망 보안 통합 플랫폼 신설

기관 간의 원문 데이터 이동에 따른 개인정보 및 영업비밀 유출을 방지하기 위해 각 제도

창구(UNI-PASS, KISA 포털 등)에 저장된 증빙을 이동하지 않고, 메타데이터만 공유하는 Zero-copy 방식의 공급망 보안 통합 플랫폼을 구축한다. 플랫폼은 공통 심사 기준 5개(접근통제/로그/외부자/운영보안[취약점·패치]/자산·구성[SBOM])에 한정해 작동하며, 개인정보보호법의 목적 제한, 최소 수집 원칙을 준수한다. 모든 열람, 적용 내용은 감사 가능하도록 기록하고, 상호인정 수준에 따라 3단계로 (인증 간소화 - 대체 - 조건부 적용) 차등 적용한다.



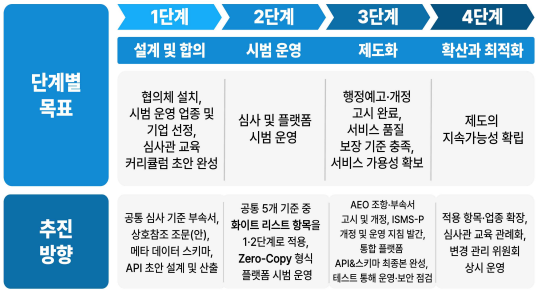
[그림 1] 아키텍처

기업은 AEO·ISMS-P·SBOM 관련 증빙 원문을 내부에서 관리하며, 표준화된 검증 시스템을 통해 메타 데이터 기반으로 각 인증 포털과 상호검증한다. AI 기반 리포트는 SBOM 데이터를 활용하여 EOL/EOS 위험도와 취약점, 대응 계획 등을 자동 분석하고 그 결과를 기업 및 심사기관에 전달한다.

각 기관은 고유 권한 내에서 역할을 수행하며, 관세청은 AEO 총괄, KISA·개인정보위는 ISMS-P 기준 및 서식 관리, 과기정통부·KISA는 SBOM 표준 관리와 운영 가이드 관리, 운영기관은 플랫폼의 전체적인 운영과 보안·키·감사를 담당한다. 사후 검증은 자동 무결성 검사와 표본 검증(연 10% 이상)을 병행하며, 위반 발생 시 전수 재검증 또는 상호참조 중단을 적용한다.

3. 시행 전략

본 정책은 다음과 같은 4단계 로드맵에 따라 추진할 수 있다. 각 단계는 기관별 역할 분담과 병행 운영이 가능하도록 설계하며, 특히 2단계에서는 기술적 실증과 행정 절차적 검증을 동시에 시범 운영 및 진행한다.



[그림 2] 정책 추진 로드맵

Ⅳ. 결론

본 논문은 글로벌 공급망 보안의 주요 위협 요인인 EOL/EOS 사용과 기존 인증 제도의 기술적 공백 및 중복 심사 문제를 해결하기 위해, SBOM 기반의 연계형 공급망 보안 관리 모델을 제시하였다.

SBOM을 활용해 EOL/EOS와 취약점을 검증하여 ISMS-P를 기술 중심의 예방 체계로 확장하고, AEO에 사이버 보안 조항을 신설하여 물리적·디지털 공급망을 통합 관리한다. 또한, 제도 간 공통 심사 기준과 메타데이터 기반 통합 플랫폼을 구축하여 효율성과 정보 보호를 동시에 확보한다.

이를 통해 기업은 보안 투자 효율을 높이고 정부는 행정 자원을 절감하며, 대한민국은 관리적 신뢰와 기술적 투명성을 결합한 새로운 공급망 보안 표준을 선도할 수 있다.

[참고문헌]

[1] 보안뉴스. (2025.08.11). 예스24, 두달 만에 또 랜섬웨어 공격 … “시스템 긴급 차단 후 복구 중”.

[2] 관세청. (2024). 수출입안전관리우수업체(AEO) 제도 안내. https://www.customs.go.kr

[3] 과학기술정보통신부·개인정보보호위원회·한국인터넷진흥원. 「정보보호 및 개인정보보호 관리체계 인증기준 고시」, 제2023-10호.

[4] 과학기술정보통신부·국가정보원·디지털플랫폼정부위원회. (2024). 「SW 공급망 보안 가이드라인」.