글로벌 공급망 보안 규제 프레임워크 동향 분석

김원빈[1], 이지언[2], 김정연[3], 유진호[3], 서대희[4]
[1]상명대학교 융합보안연구소 부소장
[2]상명대학교 컴퓨터과학과 석사과정
[3]상명대학교 경영학부 교수
[4]상명대학교 지능데이터융합학부 교수
binn.kim29@gmail.com, jiun000419@gmail.com,
jykim@smu.ac.kr, jhyoo@smu.ac.kr, daehseo@smu.ac.kr

An Analysis of Global Supply Chain Security Regulatory Frameworks

Won-Bin Kim[1], Jieon Lee[2], JeongYeon Kim[3], JinHo Yoo[3], DaeHee Seo[4]
[1]Advanced Research Center of Convergence Security, Sangmyung University
[2]Dept. of Computer Science, Sangmyung University
[3]Dept. of Business Administration, Sangmyung University
[4]Dept. of Intelligent Data Convergence, Sangmyung University

요 약

글로벌 소프트웨어 공급망의 보안 중요성이 커짐에 따라 주요 국가들은 다양한 규제 프레임워크를 도입하고 있다. 미국은 행정명령(EO 14028, 14144, 14306)과 EU는 법령(CRA, NIS2, DORA)을 중심으로 규제 대상, 핵심 요구사항 및 법적 강제력을 제공하고 있다. 본 연구에서는 미국, 유럽연합(EU), 한국의 공급망 보안 관련 법·제도 동향을 비교·분석하였다. 또한, 분석 결과를 기반으로 국내에서도 SBoM 의무화, 공공조달 보안 요건 강화 등 글로벌 추세에 부합하는 정책 보완이 필요함을 제시한다.

1. 서론

디지털 시대에 소프트웨어 공급망(Security Supply Chain)은 사이버보안의 핵심 요소로 부각되고 있다. 오늘날 한 조직이 사용하는 소프트웨어에는 수많은 오픈소스 라이브러리와 제3자 구성요소가 포함되며, 이들의 취약점을 악용한 공급망 공격이 증가 추세에 있다. 대표적으로 2020년 발생한 SolarWinds 해킹 사태는 신뢰받는 소프트웨어 업데이트 체계가 침해되어 전 세계 수만 개 조직에 파급된 사례로, 공급망 보안의 취약성을 드러냈다. 이러한 연쇄적인 공급망 기반의 대형 공격 이후 각국 정부는 소프트웨어 개발부터 배포에 이르는 전 단계의 보안 강화 방안을 모색하기 시작했다.

공급망 보안 위협에 대응하여 미국과 EU(European Union)를 중심으로 사이버보안 규제를 한층 강화하는 움직임이 나타났다. 미국은 국가안보 차원에서 연방 정부가 사용하는 소프트웨어의 보안을 높이기 위해 일련의 행정명령을 발표하였으며, EU는 내부 시장과 소비자 보호를 위해 사이버보안 관련 법률 (NIS2 지침(Network and Information Security Directive v2), DORA(Digital Operational Resilience Act) 규정, 사이버 복원력법(CRA, Cyber Resilience Act) 등)을 제정하였다[1-3]. 미국의 행정명령은 SolarWinds 사태 이후 연방 조달망에 엄격한 보안 요건(SBoM(Software Bill of Material) 공개, 보안개발 프로세스 준수 등)을 부과하였고, EU 역시 핵심 기반시설과 디지털 제품의 보안 수준을 법적으로 강제하는 방향으로 전환하고 있다.

본 연구의 2장에서는 미국과 EU의 주요 공급망 보안 규제 프레임워크의 내용과 특징을 살펴보고, 3장에서는 이를 토대로 한국 정책에 대한 시사점을 도출한다. 그리고 4장에서는 결론으로 마무리한다.

2. 글로벌 공급망 보안 법제도 동향

2.1 미국: 연방 행정명령(EO)을 통한 공급망 보안 강화

미국 바이든 행정부는 2021년 5월 행정명령 14028호(EO-14028)를 통해 연방정부 소프트웨어

공급망 보안 강화를 위한 종합 조치를 시작하였다[4]. 이 행정명령은 연방 기관이 도입하는 소프트웨어에 대해 SBoM 제출, 안전한 소프트웨어 개발 체계 준수 증명(Attestation) 요구, 취약점 보고 및 패치 프로세스 마련 등을 핵심 내용으로 담고 있다. 이에 따라 NIST(National Institute of Standards and Technology는 SSDF(Secure Software Development Framework)를 제정하여 안전한 개발 관행을 제시하였고, 연방 기관과 계약하는 소프트웨어 공급업체는 해당 기준을 준수함을 증명해야 한다[5]. 2025년 1월에는 행정명령 14144호(EO-14144)가 추가 발표되어 공급망 위험관리(C-SCRM, Cyber Supply Chain Risk Management), 양자내성암호(PQC, Post Quantum Cryptography) 준비, IoT(Internet of Things) 보안 라벨(Cyber Trust Mark) 도입 등 미래 위협 대응까지 범위를 넓혔다[6]. 이어 2025년 6월 출범한 차기 행정부는 행정명령 14306호(EO-14306)를 통해 이전 조치를 일부 개정·재구성하면서, NIST에 SSDF 업데이트와 연방조달규정(FAR, Federal Acquisition Regulation) 개정 작업에 대한 구체 일정을 부여하여 정책 이행력을 강화하였다[7]. 이로써 미국은 연방 정부 조달계약에 공급망 보안 조건을 명문화하고, 이를 위반하는 업체는 계약상 불이익을 받는 강력한 간접 제재 체계를 구축하였다.

2.2 EU: 사이버보안 법령을 통한 민간 부문 규제

유럽연합은 2022년 NIS2 지침을 채택하여, 에너지·교통·의료·공공 등 중요 분야의 필수 기관 및 중요 기관을 대상으로 사이버보안 관리체계 구축을 의무화하였다[1]. NIS2는 각 기관에 사이버 위협 위험관리 조치 수립, 공급망 보안 강화, 심각한 사고 발생 시 24시간 이내 통지 등을 요구하고, 이행하지 않을 경우 최대 1,000만 유로(또는 매출 2%)의 과징금을 부과할 수 있다. 같은 해 제정된 DORA는 금융권(은행, 보험, 투자사 등)과 그들의 ICT 서비스 제공업체를 대상으로 한 규제로, 금융사의 ICT 리스크 관리체계 구축, 중대 ICT 사고 보고, 주기적 디지털 복원력 테스트(예: 침투테스트), 제3자 공급업체 리스크 관리 등을 의무화하였다[2]. DORA 위반 시에는 금융 감독당국이 시정 명령과 제재를 부과할 수 있어, 금융 부문의 공급망 보안 수준을 높이는 역할을 한다.

<표 1> 미국, EU, 한국의 공급망 보안 규제 프레임워크 핵심 요소 비교

구분	미국 (행정명령 14028/14144/14306)	EU (CRA 법령, NIS2 지침, DORA 등)	한국 (현행 법/지침)
규제 대상	• 연방 정부 및 연방 조달 계약 대상 소프트웨어 공급업체 (정부 조달망 중심)	• EU 시장에 출시되는 모든 디지털 제품 (CRA) • 필수 서비스 제공자 및 중요 기관 (NIS2) • 금융기관 및 ICT 공급업체 (DORA)	• 주요정보통신기반시설 운영자 (일부 법률)공공 부문 정보시스템 개발사업 등일반 기업 대상 직접 규정은 없음
주요 요구사항	• 안전한 소프트웨어 개발 관행 준수 증명(attestation) • SBoM 제출 및 취약점 대응 프로세스 구축 • 연방 조달 계약에 보안 요건 포함 (FAR 개정 진행) • IoT 제품 보안 라벨 부착 (향후 연방조달에 필수)	• 보안 설계 및 기본 보안설정 적용 • 취약점 관리와 보안 업데이트 제공 (수명주기 보안) • 중대 사고 24시간 내 통보 • 주기적 보안 테스트/감사 및 제3자 리스크 관리 (DORA)	• 정보통신망법: 제품 취약점 발생 시 조치 권고 • 정보통신기반 보호법: 중요시설 장비 도입 시 안전성 검토 • 전자정부법 지침: 개발단계 시큐어코딩 적용 및 취약점 점검 • SW진흥법: 안전한 SW 개발 역량 진흥 (권고 수준)
SBoM 요구	• 연방정부 조달 소프트웨어에 SBoM 제출 의무 • NTIA가 정의한 SBoM 최소 요소 기반 (민간 부문은 자율 권장)	• CRA에 따라 모든 해당 제품에 SBoM 작성 · 유지 의무 • 제품 CE 인증 시 SBoM 포함하여 제출 • NIS2/DORA에서는 SBoM 직접 언급은 없음	• KISA 가이드라인을 통해 SBoM 작성 권고일부 산업(의료, 에너지 등) 시범사업 추진법적 의무 아님 (자율 도입 단계)
보안 개발프레임 워크	• NIST SSDF(SP 800-218) 준수 요구소프트웨어 개발 보안활동 Attestation 제출 • 연방정부 계약조건에 SSDF 반영, 지속 개선	• 별도 명문화된 프레임워크 없음 → 대신 Secure by Design 원칙을 법제화 (CRA) • 필수 서비스 분야는 ENISA 지침 등 준거 (NIS2)	• 행정기관 개발보안 가이드라인 존재 (시큐어코딩 기준)민간에는 OWASP 등 모범사례 보급 수준SW 개발보안 교육/훈련 위주 지원
법적 강제성	• 행정명령 기반: 연방조달계약상 의무 → 불이행 시 정부조달 참여 제한민간 전체에 직접 강제력은 없음	• EU 법령 직접 적용: 위반 시 과징금, 판매금지 등 제재 • CRA 불이행 제품은 시장 접근 제한 (CE 마크 불허)	• 법률상 명시적 제재조항 거의 없음 • 권고나 행정지도로 운영되는 경우가 많음(예: 인증 · 점검 미이행 시 처벌 조항 부재)

2024년 EU에서 최종 합의된 CRA은 범용 소프트웨어·하드웨어 제품의 사이버보안을 직접 규제하는 획기적인 법안이다[3]. CRA는 유럽시장에 판매되는 모든 디지털 요소 제품(PDE, Products with Digital Elements)에 대해 제조사와 수입업자 등에 일정 사이버보안 요건 준수를 의무화하며, 보안 내재화(Secure-by-design), 취약점 관리 및 보안 업데이트 제공, SBoM 작성 및 기술문서 비치 등의 요구사항을 규정하고 있다. 제조사는 제품 출시 전에 이러한 요건에 따라 제품을 평가하고 CE 마크를 획득해야 하며, 심각 취약점 발생 시 24시간 내에 EU 당국에 신고해야 한다. CRA를 위반하는 제품은 리콜되거나 EU 시장 판매가 제한될 수 있으며, 최대 1,500만 유로 또는 매출의 2.5%까지 과징금이 부과된다. 한편, CRA는 오픈소스 소프트웨어 프로젝트와 같이 영리 목적이 아닌 소프트웨어는 규제 대상에서 제외하여(오픈소스 예외) 혁신에 미치는 영향을 완화하고 있다.

2.3 미국·EU의 법제도 현황 비교

미국과 EU의 조치를 비교하면 <표 1>과 같으며, 미국은 연방 정부 조달을 매개로 한 계약 기반 규제, EU는 법령을 통한 시장 전체 규제로 접근한다. 미국 행정명령은 법률이 아니지만 연방 계약 참여 기업에는 사실상 강제력이 있다. EU의 NIS2, DORA, CRA는 법적 의무를 부과하고 위반 시 과징금·시장 퇴출 등 강력한 제재로 이행을 확보한다. SBOM의 경우 미국은 연방정부 사용 소프트웨어에 제출을 의무화해 민간 확산을 유도하고, EU는 CRA로 모든 유통 제품에 요구한다. 개발 보안 측면에서 미국은 NIST SSDF를 조달 조건에 적용·업데이트하며, EU는 별도 프레임워크 대신 CRA로 보안 내재화를 강제한다. 요약하면, 양측 모두 공급망 보안 강화를 지향하지만 적용 범위와 이행 방식은 다르다.

4. 국내 공급망 보안 법제도 시사점

현재 우리나라에는 공급망 보안에 특화된 개별 법률은 존재하지 않지만, 관련된 일부 법·제도가 부분적으로 적용되고 있다. 주요 법령들의 현황을 보면 다음과 같다:

- **정보통신망법:** 정보통신망 연동 기기·소프트웨어의 취약점 관리 조항을 두고 있으나, 제조사·개발자 대상 보안 인증이나 사전 승인 제도는 없다. 취약점 발견 시 개선 권고와 이용자 통지 의무가 있으며, 과기정통부는 취약점 신고 포상제를 운영해 민간 제보를 장려한다.

- **정보통신기반 보호법:** 주요정보통신기반시설 운영자는 정기 취약점 분석·평가와 보호대책 수립이 의무이며, 장비·시스템 도입 시 보안성 검토를 통해 공급망 위험을 사전 점검한다.

- **소프트웨어 진흥법:** 소프트웨어 개발 보안 조항이 있으나 강제성은 없고, 정부가 연구·인력양성·지원사업을 추진해 안전한 개발활동을 촉진한다. 가이드라인 배포와 교육 중심이며 민간 직접 규제는 아니다.

- **전자정부법 및 지침:** 행정기관·공공기관의 정보시스템 구축 시 시큐어코딩, 취약점 점검 등을 요구하는 지침이 적용된다. 공공 조달의 공급망 보안을 확보하지만, 행정규칙 수준에 머문다.

이처럼 한국은 일부 법률과 지침을 통해 공급망 보안을 부분적으로 다루고 있지만, SBoM 제출 의무화나 보안 인증 등 국제적 수준의 포괄적 규제는 아직 도입되지 않았다. 대신 정부 주도로 2022년부터 소프트웨어 공급망 보안 강화 태스크포스(TF)를 운영하고, 한국인터넷진흥원(KISA) 주관의 SW 공급망 보안 가이드라인을 배포하는 등 정책적 기반 마련에 집중하고 있다. 또한 전자정부 사업을 대상으로 SBoM 시범사업을 추진하고 국제 표준(SPDX, CycloneDX 등) 적용을 시험하는 단계이다.

앞서 살펴본 글로벌 규제 동향을 고려할 때, 한국에는 다음과 같은 법·제도 보완이 시급하다고 판단된다:

- **핵심 분야 제품 보안 요구사항 법제화:** 미국의 행정명령과 EU CRA처럼, 정부기관·공공부문 및 중요 기반시설에 납품되는 디지털 제품에 대해 SBOM 제출, 취약점 대응 체계 등 보안 요건을 법적으로 의무화할 필요가 있다. '디지털제품 보안확보 및 공급망 보호법(가칭)'을 제정해 공공조달 소프트웨어와 IoT 기기의 최소 보안 기준을 명시함으로써, 기존 권고 중심의 가이드라인에 실효성을 부여할 수 있다.

- **SBOM 활용의 제도적 기반 마련:** 글로벌 추세에 맞춰 SBOM 제출을 법제화해야 한다. 의료기기, 산업제어시스템, 공공 SW 조달 등 위험도가 높은 분야부터 단계적으로 적용하고, 향후 범위를 확대하는 방식이 바람직하다. 이를 위해 정보통신망법이나 전자정부법 시행령에 관련 조항을 신설하고, SPDX·CycloneDX 등 국제 표준을 적용해 구성요소 투명성을 높임으로써 제3자 취약점 대응 역량을 강화해야 한다.

- **공공조달 계약의 보안조건 강화:** 정부 및 공공기관의 IT 사업 계약에 보안 요구사항을 명문화하고 미준수 시 제재할 근거를 마련해야 한다. 현재 일부 지침 수준에 머문 시큐어코딩, OWASP 대응 요구를 국가계약법 등 상위 규정에 반영하고, 대규모 프로젝트에는 SSDF 기반 개발체계와 제3자 보안 감사 의무화를 고려함으로써 미국 연방조달 규정과 유사한 효과를 낼 수 있다.

- **IoT 제품 보안인증 제도 도입:** 스마트홈, 의료, 산업용 IoT 등 사이버위험이 큰 제품군에는 보안 인증·라벨링 제도를 도입해야 한다. EU는 CE 마크에 사이버보안 적합성 요건을 포함했고, 미국도 Cyber Trust Mark를 운영 중이다. 한국도 KC 인증에 보안 항목을 추가하거나 별도 IoT 보안 인증제를 마련해 시장 유통 전 최소 보안요건을 확보하고, 동시에 해외 규제 대응 및 수출 경쟁력을 높일 수 있다.

- **기업의 규제 대응 역량 지원:** 글로벌 규제 준수를 위해 기업이 SBOM 생성·관리, SSDF 실천, CRA·EO 대응 역량을 확보하도록 교육·컨설팅과 자동화 도구를 지원해야 한다. 또한 규제 대응 프로젝트 매니저(PM) 육성, 보안 조직 구축을 유도하고, 정부는 소통 창구를 통해 새 규제 정보를 공유하여 기업의 부담을 최소화해야 한다.

5. 결론

전 세계적으로 소프트웨어 공급망 보안 규제는 기존의 자율적 권고 수준에서 강제적 규범으로 빠르게 전환되는 추세이다. 미국의 연방 조달 규칙 강화, EU의 사이버보안 법제 신설 등은 모두 공급망에 존재하는 취약점을 사전에 제거하고 신뢰성 있는 디지털 생태계를 구축하려는 노력으로 볼 수 있다. 이러한 규제 흐름 속에서 한국의 기업과 정부는 선제적으로 대응 전략을 마련해야 한다. 기업은 글로벌 시장에서 생존하기 위해 자사 제품과 서비스가 국제 보안 기준을 충족하는지 점검하고 개선해야 한다. 예를 들어 유럽에 제품을 수출하려는 제조기업은 CRA의 CE 마크 요건을 충족하기 위한 보안 조치를 사전에 갖추어야 하며, 미국 연방기관과 거래하는 IT 기업은 NIST 기준의 보안 개발체계를 내재화해야 한다. 정부도 국내 제도가 글로벌 스탠더드와 정합성을 이루도록 지속적으로 개선할 필요가 있다. 앞서 제시한 법제도 개선과 더불어, 국제 공조를 통해 우리 기업의 보안 인증이나 SBoM 등이 해외에서 상호 인정받을 수 있는 체계를 구축해야 할 것이다.

사사표기

이 논문은 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원-대학ICT연구센터(ITRC)의 지원을 받아 수행된 연구임(IITP-2025-RS-2024-00438056)

참고문헌

[1] European Commission, Directive (EU) 2022/2555 (NIS2 Directive), Brussels, 2022.
[2] European Commission, Regulation (EU) 2022/2554 (DORA: Digital Operational Resilience Act), Brussels, 2022.
[3] European Commission, The Cyber Resilience Act (CRA), Regulation (EU) 2024/XXXX, Brussels, 2024.
[4] The White House, Executive Order 14028: Improving the Nation's Cybersecurity, Washington, D.C., 2021.
[5] NIST, Secure Software Development Framework (SSDF), SP 800-218, Gaithersburg, MD, National Institute of Standards and Technology, 2022.
[6] The White House, Executive Order 14144: Advancing Cybersecurity and Supply Chain Risk Management, Washington, D.C., 2025.
[7] The White House, Executive Order 14306: Federal Acquisition Regulation (FAR) Updates for Software Security, Washington, D.C., 2025.