방산안보연구
Journal of Defense Industrial Security

방산안보연구, 2권 1호, 2026년 3월, 19-46면.
Journal of Defense Industrial Security, Volume 2, Issue 1, March 2026, Pages 19-46.
https://doi.org/10.64227/jdis.2026.2.1.2

Print ISSN 3091-5546
Online ISSN 3091-5554

원저

소프트웨어 공급망 보안의 규제화와 방위산업 대응 전략: EU CRA 2027년 시행을 중심으로 방산업체와 기업의 대응 전략

김찬우

제이제이시스템 대표

교신저자: 김찬우 (jj.system.kr@gmail.com)

요약

소프트웨어 공급망 보안이 국방 산업과 개인정보 보호의 핵심 요소로 부상하면서 국제적 규제화가 가속화되고 있다. 본 연구는 2024년 발효된 사이버 복원력법(CRA, Cyber Resilience Act)의 2027년 본격 시행을 중심으로, EU의 일반개인정보보호법(GDPR, General Data Protection Regulation) 시행(2018년 5월) 이후 CMS Law가 운영하는 GDPR Enforcement Tracker에서는 2025년 1월까지 누적된 약 56억 5천만 유로의 과징금 사례와 소프트웨어 자재명세서(SBOM, Software Bill of Materials) 기반 규제 대응 전략을 분석하며 단기 대응 전략을 제시한다. 특히 국내 소프트웨어 개발자 350명을 대상으로 한 실증 조사에서 드러난 인식-행동 격차(awareness-behavior gap, ABG)를 분석하여, 기업·정부·개발자 차원의 다층적 대응 전략을 제시한다. 연구 결과, 개발자들의 SBOM 필요성 인식과 실제 구현 역량 간 격차가 확인되었으며, 특히 조직 지원 부족이 가장 심각한 장애 요인으로 확인되었다. 본 논문은 GDPR 규제 미준수 사례로부터의 교훈을 적용하여 CRA 2027년 시행까지 남은 기간에 국내 방산업체와 개발자가 취해야 할 구체적 대응 로드맵을 제시하며, 국방·보안 산업을 중심으로 한 정책적 시사점을 도출한다.

핵심어

소프트웨어 공급망 보안, SBOM, 사이버 복원력법, GDPR, 규제 준수, 개발자 역량, 방산보안

차례

접수일: 2026년 2월 3일
수정일: 2026년 2월 19일
게재승인일: 2026년 3월 10일
출판일: 2026년 3월 31일

Original Article

Regulatory Evolution of Software Supply Chain Security and Defense Industry Response Strategy: Focused on EU CRA's Full Implementation in 2027

Chanwoo Kim

CEO, J.J.System, Republic of Korea

Corresponding Author: Chanwoo Kim (jj.system.kr@gmail.com)

ABSTRACT

As software supply chain security has emerged as a core element of both defense capability and personal data protection, regulatory enforcement at the international level is rapidly accelerating. This study focuses on the Cyber Resilience Act (CRA), which entered into force in 2024 and will be fully enforced from 2027, and examines approximately EUR 5.65 billion in cumulative GDPR-related administrative fines recorded up to January 2025 in the GDPR Enforcement Tracker operated by CMS Law, in order to analyze Software Bill of Materials (SBOM)–based regulatory response strategies and propose short-term compliance measures.

Drawing on an empirical survey of 350 domestic software developers, the study investigates the awareness–behavior gap (ABG) in SBOM adoption and derives multilayered response strategies at the levels of firms, government, and individual developers. The results confirm a substantial gap between developers' perceived necessity of SBOM implementation and their actual implementation capability, with organizational support deficiency emerging as the most critical barrier.

By applying lessons learned from GDPR non-compliance cases, this paper proposes a concrete response roadmap for Korean defense contractors and software developers in the remaining period leading up to CRA's full enforcement in 2027, and derives policy implications centered on the defense and security industries.

KEYWORDS

software supply chain security, SBOM, Cyber Resilience Act (CRA), GDPR, regulatory compliance, developer capability, defense industry security

1. 서론

1.1. 연구의 배경

소프트웨어 공급망 보안(Software Supply Chain Security, SSCS)은 더 이상 기술적 선택사항이 아니라 국가 안보와 경제 안정성의 핵심 요소가 되었다[1]. 2020년 SolarWinds 공격[2]과 2021년 Log4Shell 취약점[3]은 소수의 핵심 소프트웨어 구성 요소가 얼마나 광범위한 피해를 야기할 수 있는지를 명확히 보여주었다.

미국 행정부는 2021년 Executive Order 14028을 통해 정부 조달 소프트웨어에 SBOM 포함을 의무화했으며[4], EU는 이보다 더 광범위한 규제 체계인 사이버 복원력법(CRA, Cyber Resilience Act)을 2024년 발효하여 2027년 12월부터 본격 시행할 예정이다[5]. CRA에서의 SBOM 요구는 제13조 제1항 (h) 및 부록 I Part II (1)에 근거하며, 제조자가 제품에 포함된 컴포넌트를 식별·문서화하기 위해 "일반적으로 사용되는 기계가독 형식의 SBOM"을 작성하도록 규정하고 있다.

현재 평균적인 소프트웨어 제품은 300개 이상의 오픈소스 구성 요소로 구성되어 있으며[6], 이들 각각에 대한 라이선스, 취약점, 의존성 정보를 추적하는 것은 단순한 기술 문제를 넘어 기업의 법적 리스크 관리의 핵심이 되었다.

특히 GDPR(General Data Protection Regulation)의 시행(2018년 5월) 이후 2025년 1월까지 6년 8개월간 누적된 약 56억 5천만 유로의 과징금[7]은 단순한 벌금을 넘어 기업의 평판 손상, 운영 중단, 국제 신용도 하락으로 이어진 체계적 피해를 의미한다[8]. 이 막대한 규제 비용은 개별 기업의 재무에 심각한 타격을 주었을 뿐만 아니라, 해당 기업들의 주가 하락, 고객 신뢰도 하락, 국제 거래처 이탈 등으로 확산되었다.

Meta의 경우 2023년 단 한 건의 과징금(12억 유로)만으로도 연간 순이익의 10% 이상을 상실했으며, Amazon도 약 7억 5천만 유로의 과징금으로 인해 EU 시장에서의 신뢰도가 급락했다.

한국의 관점에서 이러한 국제 규제 환경의 변화는 두 가지 차원의 긴급성을 제시한다. 첫째, 국내 소프트웨어 수출 기업들이 EU 시장 진출 시 CRA 준수가 필수 조건이 될 것이라는 점이고[9], 둘째, 국방·보안 산업의 공급망 투명성 요구가 국제적으로 강화되고 있다는 점이다[10]. 따라서 현 시점(2026년)에서 기업과 개발자의 선제적 준비는 단순한 규제 대응을 넘어 국제 경쟁력 강화의 관점에서 필수적이다.

1.2. 연구의 의의 및 목적

본 연구는 다음의 세 가지 핵심 질문에 답하고자 한다.

첫 번째 연구 질문: GDPR 규제 실패로부터 어떤 교훈을 도출할 수 있는가?

GDPR은 데이터 보호 규제의 '글로벌 표준'으로 자리 잡았으나, 시행 초기 많은 기업들의 준비 부족으로 인한 과징금 누적은 규제 대응의 '타이밍'이 얼마나 중요한지를 보여준다. GDPR 시행 전(2015-2017년) 충분한 기술·조직적 준비를 하지 못한 기업들은 시행 이후 막대한 추가 비용을 부담해야 했다[11].

특히 Paul Hastings 설문(2018)에서 영국 상장 기업(FTSE 350)의 94%, 미국 대기업(Fortune 500)의 98%가 준수 준비를 주장했으나, 실제로는 내부 태스크포스 구성(39-47%), 갭 분석(1/3), 컨설턴트 고용(1/3) 등 핵심 조치가 미흡해 과신된 상태로 드러났다.

또한 SecurityMetrics 설문(2018)에서 영국 기업 평균 준비도는 54%였으나, 이는 2018년 초 기준으로 여전히 낮은 준수율을 시사하며, 30%대 준비 기업이 다수였다.

AlertLogic 보고서(2018)에서는 전체 기업 중 완전 준수 7%, 진행 중 33%로 60%가 마감 미달 가능성을 보였다.

또한 국내에서는 준비도에 대한 자료들이 부족하나 국민권익위원회 보고서(2021)에서 KISA GDPR 위반 사례 분석 (2018~)을 통해 GDPR 위반 사례(적법 처리 근거 부족 60%)를 분석하며 한국 기업 리스크 관리를 강조했다. EU 적정성 결정(2021) 전후 자료에서 한국 기업의 준수 노력(표준계약조항 등)이 부각되지만, 초기 준비 미달로 EU 시장 진출 비용 증가가 문제로 지적되었다.

이러한 자료들은 시행 초기(2018) 한국 기업 평균 준비도가 30-50% 수준에 불과하다는 것을 뒷받침한다. 2018년 규제 발효 당시 기업들이 가진 평균 준비도는 30% 수준에 불과했으며, 이로 인해 발효 후 첫 2년간 긴급 대응에만 많은 비용을 소비해야 했다. 이러한 패턴을 CRA 대응에서 반복하지 않기 위해서는 GDPR 사례로부터의 명확한 교훈 도출이 필수적이다.

두 번째 연구 질문: 현재 개발자와 기업의 SBOM 채택 의도와 실행 능력 간의 격차는 어느 정도인가?

선행 연구에 따르면 환경 문제(예: 기후 변화)에 대한 인식-행동격차(awareness-behavior gap -ABG)가 상당하다는 것이 알려져 있다[12]. 본 연구는 SBOM 채택이라는 구체적인 기술 정책 맥락에서 이러한 격차가 존재하는지, 그리고 그 크기가 어느 정도인지를 실증적으로 파악하고자 한다. 특히 한국의 소프트웨어 개발자들이 SBOM의 필요성을 충분히 인식하고 있음에도 불구하고, 실제 조직 현장에서의 구현이 진행되지 않는 이유를 규명하는 것이 중요하다.

세 번째 연구 질문: CRA 2027년 12월 본격 시행까지 남은 기간에 한국 기업과 개발자가 취해야 할 구체적 대응 전략은 무엇인가?

규제가 예정되어 있을 때, 선제적 대응 여부가 기업의 피해 규모를 결정한다[13]. 따라서 현 시점(2026년 1월)에서 CRA 2027년 시행까지의 구체적 로드맵을 제시하는 것은 기업과 개발자의 실질적 의사결정을 지원하는 데 중요한 역할을 할 것이다. 본 연구에서는 기업 규모별, 산업별, 역할별로 세분화된 실행 전략을 제시함으로써, 한국의 소프트웨어 산업 전체가 선제적으로 국제 규제에 대응할 수 있는 기초를 마련하고자 한다.

2. 이론적 배경

2.1. GDPR의 규제 체계와 과징금 분석

2.1.1. GDPR의 규제 구조

2018년 5월 발효된 GDPR은 EU 역내 개인정보 처리에 관한 규정을 획기적으로 강화했다[14]. GDPR의 가장 특징적인 요소는 글로벌 연매출의 최대 4%까지 과징금을 부과할 수 있다는 점이며, 이는 CCPA와 같은 다른 규제와 비교하면 훨씬 가혹한 수준이다.

GDPR은 2단계의 위반 수준을 구분하여 과징금을 부과한다.

먼저 1단계 위반으로는 글로벌 연매출의 2% 또는 1천만 유로 중 큰 액수를 부과하며, 이러한 위반에는 불충분한 보안 조치, 기록 미유지, 취약점 신고 지연 등이 해당된다.

다음으로 2단계 위반으로는 글로벌 연매출의 4% 또는 2천만 유로 중 큰 액수를 부과하는데, 이는 법적 근거 부족, 동의 획득 실패, 개인 권리 침해 등 보다 심각한

위반을 대상으로 한다. 이러한 차등적 과징금 체계는 규제 당국이 기업의 위반 행위의 심각성을 직접적으로 재정에 반영하려는 의도를 보여주며, 단순한 벌금이 아니라 기업의 경영 전략 자체를 변화시키도록 설계되었다.

2.1.2. GDPR 과징금 현황(2018.05-2025.01)

GDPR 시행 이후 누적 과징금 통계를 분석하면 매우 흥미로운 패턴이 드러난다. 이는 서로 다른 트래커 기준으로 분석한 부분이다[7,15].

2018년 5월부터 2025년 1월까지 누적된 총 과징금은 약 56억 5천만 유로에 이르며, 이는 약 2,245건의 개별 사건에 의한 결과이다. 건당 평균 과징금은 약 236만 유로지만, 이 수치는 소수의 초대형 과징금에 의해 큰 영향을 받으며, 건당 최고액은 Meta가 2023년에 받은 12억 유로에 달한다.

연도별 추이를 살펴보면 규제 집행의 가속화 추세가 명확하게 드러난다. 2018년에는 약 1억5천만 유로에 불과했던 누적 과징금이 매년 급격하게 증가하여 2023년에는 약 267억 유로에 이르렀다. 이는 2018년 대비 180배 규모의 증가이며, 연평균 증가율로 환산하면 매년 50% 이상씩 증가하고 있다는 의미이다. 특히 2022년과 2023년 사이의 증가율이 가장 급격한데, 이는 규제 당국이 2020년대 초반부터 본격적으로 대규모 기업을 대상으로 집행을 강화했음을 시사한다.

이러한 과징금 증가율의 가속화는 세 가지 중요한 의미를 갖는다.

첫째, 규제 당국의 단속 강화가 단순한 초기 움직임이 아니라 장기적 추세라는 점이다. 초기 유예 기간이 끝나고 본격적인 감시체계가 구축된 이후, 매년 규제 집행의 강도가 높아지고 있다.

둘째, 대규모 기업의 위반 적발이 증가하고 있다는 점인데, 누적 과징금의 70% 이상이 상위 20개 사건에서 발생하고 있으며, 이들은 모두 글로벌 기술 대기업이나 국제 플랫폼 기업들이다[16]. 이는 규제 당국이 영향력이 큰 기업들을 우선적으로 대상으로 삼고 있음을 의미한다.

셋째, 기업들의 규제 대응이 여전히 미흡하다는 점이다. 규제 시행이 이미 6년 이상 진행되었음에도 불구하고, 과징금이 계속 증가하고 있다는 것은 기업들이 GDPR 준수를 위해 실질적인 변화를 이루지 못하고 있다는 것을 암시한다.

2.1.3. 주요 위반 사례 분석

2.1.3.1. Meta (메타/페이스북)의 복수 위반 사례

Meta는 GDPR 시행 이후 여러 건의 과징금을 부과받았으며, 각 사건은 서로 다른 위반 유형을 대표한다. 먼저 2023년 아일랜드 데이터보호청으로부터 받은 12억 유로의 과징금은 Schrems II 사건으로 알려진 국제 데이터 이전 규정 위반에 대한 것이다. 이 사건은 Meta가 EU에서 수집한 사용자 데이터를 미국으로 이전할 때 충분한 법적 근거를 마련하지 않았다는 점에서 역대 최대 규모의 과징금이 되었다.

또한 2022년에는 약 4억 유로의 과징금을 받았는데, 이는 Instagram과 Facebook 사용자 데이터를 결합하는 과정에서 사용자의 동의 없이 진행한 위반에 대한 것이었다. 추가로 2024년에는 2018년 데이터 유출 사건(2,900만 계정이 노출됨)에 대한 후속 조사로 2억5천만 유로의 과징금을 받아, 같은 사건으로 인해 단계적으로 과징금이 누적되는 형태를 보여주었다.

Meta의 사례에서 도출할 수 있는 핵심 교훈은 다음과 같다.

첫째, 글로벌 대기업이라도 개인정보 처리의 법적 근거가 부족하면 막대한 과징금을 피할 수 없다는 점이다. Meta는 규모 면에서 세계 최대의 기술 기업 중 하나이지만, 규제 당국은 기업의 규모에 관계없이 법률 위반에 대해 엄격하게 대응했다.

둘째, 국제 데이터 이전 규정 준수가 GDPR에서 가장 심각한 위반 요소라는 점이다. Schrems II 사건은 EU-US 간의 데이터 이전 협약(Privacy Shield)이 무효화되면서 기업들의 국제 데이터 처리 방식에 대한 근본적인 재검토를 촉구했다.

2.1.3.2. Amazon (아마존)의 쿠키 동의 미흡 사건

Amazon은 2021년 룩셈부르크 데이터보호 당국으로부터 약 7억 5천만 유로의 과징금을 받았다. 위반 사항은 매우 구체적이었다. Amazon의 웹사이트 방문자들이 쿠키 설정에 동의하지 않았음에도 불구하고, Amazon은 광고 추적 목적의 쿠키를 무단으로 설치했던 것이다. 이 사건은 기술적으로는 간단한 구현이 가능했던 조치이지만, 법적으로는 명확한 위반이었다는 점에서 중요한 교훈을 제공한다. 규제 당국의 입장은 분명했다. 기술적으로 가능하다고 해서 법적으로 허용되는 것은 아니며, 사용자의 명확한 동의 없이 개인정보를 처리하는 행위는 GDPR의 가장 기본적인 원칙에 위배된다는 것이다. 이는 기업의 기술 개발 과정에서 법적 검토의 중요성을 강조하는 사례이다.

2.1.3.3. LinkedIn (링크드인)의 광고 추적 위반

LinkedIn은 2024년 아일랜드 데이터보호청으로부터 약 3억 유로의 과징금을 받았다. 위반 사항은 광고 목적으로 개인정보를 무단으로 처리한 것이었다. LinkedIn은 사용자들의 명시적 동의 없이 그들의 브라우징 행동 데이터를 광고 타게팅에 사용했으며, 이는 GDPR의 동의 원칙에 명백히 위배되었다.

2.1.3.4. 사례의 공통점과 교훈

모든 사례에서 관찰되는 공통적인 위반 패턴은 네 가지로 요약할 수 있다.

첫째는 법적 근거 부족(lawful basis)으로, 기업들이 개인정보를 처리할 때 충분한 법적 근거를 마련하지 않았다는 점이다. 동의가 획득되지 않았거나, 합법적 이익의 원칙이 제대로 적용되지 않았으며, 계약의 이행을 위해 필요하지 않은 데이터를 처리한 경우들이다.

둘째는 기술적 불비(inadequate security measures)로, 암호화 부족, 접근통제 미흡, 데이터 유출 시 신속한 대응 미흡 등이 포함된다.

셋째는 조직적 미흡(lack of organizational procedures)으로, DPO(Data Protection Officer) 미지정, 데이터 처리 기록 미유지, 영향평가 미실시 등이 해당된다.

넷째는 투명성 결여(transparency failure)로, 개인정보 처리 사실을 개인들에게 제때 알리지 않았거나, 명확하게 설명하지 않은 경우들이다.

이러한 패턴이 CRA 시행 시에도 반복될 것으로 예상된다는 점은 한국 기업에게 중요한 경고이다[17]. SBOM을 기반으로 한 소프트웨어 공급망 보안 규제도 유사한 논리로 작동할 것이며, 기술적 구현보다는 조직적 준비와 법적 근거 마련이 더욱 중요할 것이다.

2.2. 소프트웨어 공급망 보안의 국제 동향

2.2.1. SBOM의 개념과 국제 표준

SBOM(Software Bill of Materials)은 소프트웨어 제품을 구성하는 모든 구성 요소(components)를 명시한 형식화된 목록이다[18]. 이 개념은 물리적 제조업에서 사용되는 '부품표(BOM, Bill of Materials)'에서 유래했다. 자동차나 전자제품 제조업에서는 최종 제품이 수백 개

의 부품으로 구성되어 있으며, 각 부품의 출처, 품질, 결함 여부를 명확히 파악하는 것이 필수적이다. 마찬가지로 소프트웨어도 평균 300개 이상의 오픈소스 라이브러리와 의존성으로 구성되어 있으며, 각각의 라이선스, 취약점, 업데이트 상황을 파악해야 한다는 점에서 SBOM의 필요성이 대두되었다.

그러나 소프트웨어의 특성상 물리적 부품표와 SBOM은 몇 가지 중요한 차이가 있다.

첫째, 소프트웨어는 무형자산이므로 부품 간의 의존성이 훨씬 복잡하다. 물리적 부품은 교체 가능성이 명확하지만, 소프트웨어 라이브러리는 버전에 따라 호환성이나 보안 특성이 급격하게 변할 수 있다.

둘째, 소프트웨어는 지속적으로 업데이트되므로, SBOM도 한 번 작성하면 끝나는 것이 아니라 지속적으로 유지보수되어야 한다. 셋째, 라이선스 관계가 매우 복잡하여, 단순한 기술 정보뿐만 아니라 법적 의무까지 추적해야 한다.

SBOM이 포함해야 하는 핵심 정보 항목은 다음과 같다. 필수 항목으로는 먼저 구성 요소명(Component Name)으로, 라이브러리나 패키지의 정식적인 이름을 명시한다. 예를 들어 “log4j” 또는 “Apache Log4j”와 같은 형태이다. 다음으로 버전(Version)으로, 정확한 버전 번호를 기재하여 특정 취약점이 해당 소프트웨어에 영향을 미치는지 판단할 수 있게 한다. 또한 라이선스(License) 정보를 필수적으로 포함해야 하며, SPDX(Software Package Data Exchange) 식별자 형식을 따라야 한다. 예를 들어 “Apache-2.0”, “MIT”, “GPL-3.0” 등의 형태이다. 그리고 CVE/취약점 정보(CVE/Vulnerability)도 필수 항목으로, National Vulnerability Database(NVD)에 등재된 취약점 번호를 참조한다.

권장 항목으로는 먼저 출처(Source/Repository) 정보로, GitHub URL 등 소스코드의 위치를 명시함으로써 추가 정보를 찾거나 보안 패치를 확인할 수 있게 한다. 다음으로 해시값 체크섬(Checksum)으로, SHA-256 등의 암호학적 해시를 포함하여 다운로드한 파일의 무결성을 검증할 수 있도록 한다. 또한 종속성(Dependencies) 정보도 포함되는데, 해당 구성 요소가 의존하는 다른 요소들을 명시함으로써 간접 의존성으로 인한 취약점도 식별할 수 있게 한다.

현재 사용되는 주요 SBOM 표준은 세 가지이다. 먼저 SPDX (Software Package Data Exchange, Linux Foundation)는 가장 광범위한 수용도를 보이고 있으며, NIST에서도 권장하는 표준이다. SPDX는 JSON, XML, RDF, 스프레드시트 등 다양한 형식을 지원하며, 라이선스 정보를 중심으로 구성되어 있다. 다음으로 CycloneDX (OWASP)는 보안과 취약점 정보를 강화한 표준으로, JSON 기반의 경량화된 구조를 가지고 있으며, CI/CD 파이프라인 통합에 최적화되어 있다. 마지막으로 SWID (Software Identification Tags, ISO/IEC 19770-2)는 소프트웨어 라이선싱 관점에서 접근하는 표준으로, XML 형식을 사용한다.

CRA 2027년 시행 시 어떤 표준을 강제할 것인지는 아직 공식 발표되지 않았으나, SPDX 또는 CycloneDX 중 하나, 또는 둘 다를 요구할 가능성이 높다[19]. 이를 대비하여 한국 기업들은 현재 다중 표준 생성을 지원하는 도구 선택이 중요하다.

2.2.2. 오픈소스 생태계와 보안 위험

현대의 소프트웨어는 이전의 폐쇄형 개발 방식을 벗어나 오픈소스 생태계에 의존하는 구조로 변화했다. 평균적인 상용 소프트웨어 제품은 300~500개의 오픈소스 구성 요소로 이루어져 있으며[6], 이들 간의 의존성 깊이는 평균 5~7단계에 달한다[20]. 더욱이 주요 라이브러리는 월 1~3회 정도의 빈도로 업데이트되어[21], 개발팀이 모든 변경사항을 추적하기는 실질적으로 불가능한 상황이다.

오픈소스 보안의 주요 위험은 여러 가지 유형으로 분류할 수 있다. 먼저 직접 의존성의 취약점은 프로젝트가 명시적으로 사용하는 라이브러리에서 발견되는 결함으로, 개발팀이 상대적으로 쉽게 감지할 수 있다. 반면 간접 의존성의 취약점은 의존 라이브러리가 의존하는 요소에서 발견되는 결함으로, 발견 확률이 매우 낮다. 또한 라이선스 위반 위험도 있는데, 특히 GPL 라이센스의 의무사항을 미준수하면 법적 분쟁으로 이어질 수 있다. Supply Chain Attack은 정상적인 라이브러리가 탈취되어 악성 버전이 배포되는 경우로, 발생 빈도는 낮지만 피해가 극심하다. 마지막으로 Abandoned Project 위험으로, 유지보수가 중단된 라이브러리를 계속 사용할 경우 새로운 취약점에 대한 보안 패치를 받을 수 없다.

간접 의존성으로 인한 위험의 심각성은 2021년 12월의 Log4Shell 사건(CVE-2021-44228)에 의해 극명하게 드러났다[22]. Log4j는 Java 애플리케이션에서 광범위하게 사용되는 라이브러리였으나, 대부분의 개발자들이 자신의 프로젝트에서 직접 사용하지 않았다. 대신 다양한 오픈소스 프로젝트들이 Log4j를 간접적으로 의존하고 있었다. Log4j의 원격 코드 실행 취약점이 공개되었을 때, 직접 사용자뿐만 아니라 간접 의존자들도 즉각적인 패치를 요구받았으며, 패치가 지연된 애플리케이션들은 보안 위협에 노출되었다. 이 사건은 SBOM의 필수성을 강력하게 입증했다[23]. SBOM이 없었다면, 조직들은 자신의 소프트웨어가 정확히 어떤 라이브러리에 의존하고 있는지, 그리고 취약점이 어디까지 영향을 미치는지 파악할 수 없었을 것이다.

2.3. CRA와 SBOM 의무화

2.3.1. CRA의 규제 체계

CRA는 2024년 12월 10일 발효되었으며, 단계적인 시행 일정을 따르고 있다[5].

첫 번째 단계는 규정 발효(Immediate Application) 단계로 2024년 12월 10일부터 시작되었다. 이 단계에서는 주로 기본 요구사항들이 논의되고 기업들이 준비를 시작하는 기간이다.

두 번째 단계는 2026년 9월 10일부터 시작되는 취약점 보고 의무 단계로, 기업들이 발견한 취약점을 규제 당국에 보고해야 하기 시작한다.

세 번째이자 가장 중요한 단계는 2027년 12월 10일부터 시작되는 필수 요건 전면 시행 단계로, SBOM 제공을 포함한 모든 핵심 요구사항이 본격적으로 적용된다.

CRA의 적용 범위는 광범위하다. 적용 대상은 “디지털 요소가 포함된 제품(products with digital elements)”으로 정의되며, 이는 소프트웨어 구성 요소가 포함된 거의 모든 제품을 의미한다. 냉장고, 자동차, 의료기기, 산업 제어 시스템 등 스마트 기능이 있는 모든 제품이 포함될 수 있다. 이렇게 광범위한 정의는 EU가 디지털 기술의 보안을 얼마나 심각하게 받아들이고 있는지를 보여준다.

다만 규모가 매우 작은 마이크로 및 소기업들에 대해서는 일부 예외가 적용될 수 있으며 순수 군사용 제품은 제외되나, 방산업체에서 민간 상업적 목적과 군사적 목적 모두에 사용될 수 있는 듀얼유스(Dual-use) 제품군은 포함된다. 특히 인공지능(AI)의 경우도 포함되며 GPS나 드론도 포함되고 K-RMF의 경우도 CRA의 범위에 포함된다.

2.3.2. SBOM 의무화의 기술적·법적 함의

CRA 2027년 본격 시행 시, 모든 디지털 제품 제조업체는 구체적인 요구사항들을 이행해야 한다.

먼저 SBOM 작성 및 유지보수 요구사항으로, 제품 생산 시점부터 지속적으로 SBOM을 업데이

트해야 한다. 이는 한 번의 작성으로 끝나는 것이 아니라, 제품의 생명주기 전반에 걸쳐 지속적인 관리가 필요하다는 의미이다.

다음으로 취약점 모니터링 요구사항으로, 새로운 CVE(Common Vulnerabilities and Exposures)가 발표될 때마다 기업은 SBOM을 통해 자신의 제품에 영향을 미치는지 지속적으로 모니터링하고, Actively exploited vulnerability(활용된 취약점)가 확인될 경우 24시간 내 early warning, 72시간 내 상세 보고를 EU CSIRT(Cyber Security Incident Response Teams Network)[24] 및 ENISA(European Union Agency for Cybersecurity)[25]에 제출해야 한다(Article 14)[5]. 이는 기업으로 하여금 실시간 취약점 평가 및 보고 체계를 구축하도록 요구하는 것으로, 2026년 9월부터 적용되며 기업들에게 24/7 모니터링 체계를 갖출 것을 요구하는 것과 같다. 또한 보안 피드백 채널 제공 요구사항으로, 사용자들이 발견한 취약점을 보고할 수 있는 메커니즘을 제공해야 한다. 마지막으로 보안 업데이트 배포 요구사항으로, 식별된 취약점을 해결하기 위한 신속한 패치 배포가 필수적이다.

3. 연구 설계 및 방법론

3.1. 연구 대상 및 표본 구성

본 연구는 한국의 소프트웨어 개발자를 대상으로 온라인 설문조사를 실시했다. 연구의 신뢰성을 높이기 위해 충분한 규모의 표본을 확보하였다. 표본 규모는 총 350명의 개발자로 설정했으며, 이는 통계적 유의성을 확보하기에 충분한 규모이다.

표본 추출 방식으로는 목적적 표본 추출과 눈덩이 표본 추출을 병행했다. 목적적 표본 추출을 통해 다양한 규모의 기업(스타트업, 중소기업, 대기업)에서 근무하는 개발자들을 확보했으며, 눈덩이 표본 추출을 통해 네트워크 효과를 활용하여 표본을 확대했다. 다만 방산 업체 종사자에 대한 표본 추출에 한계가 있어 소프트웨어 개발자에 대한 해당 조사결과를 참고하였다.

조사는 2025년 9월 1일부터 12월 31일까지 4개월간 진행되었다. 조사 채널은 온라인 플랫폼들을 활용했으며, 구체적으로는 GitHub, Stack Overflow Korea, 개발자 커뮤니티 페이스북 그룹, 그리고 눈덩이 표본추출을 이용하였다. 이러한 다양한 채널의 활용은 대표성 높은 표본을 확보하는 데 도움이 되었다. 응답자의 인구통계학적 특성은 표 1과 같다.

표 1. 응답자의 인구통계학적 특성 (n=350)

특성	구분	빈도	비율(%)	누적(%)
직무	백엔드 개발자	98	28.0	28.0
	프론트엔드/모바일	76	21.7	49.7
	DevOps/SRE	42	12.0	61.7
	보안 담당자	38	10.9	72.6
	운영/인프라	56	16.0	88.6
	기타	40	11.4	100.0
경력	1년 미만	28	8.0	8.0
	1~3년	84	24.0	32.0
	3~5년	105	30.0	62.0
	5~10년	98	28.0	90.0
	10년 이상	35	10.0	100.0

고용형태	정규직	298	85.2	85.2
	계약직	32	9.1	94.3
	프리랜서	20	5.7	100.0
조직규모	대기업(1,000명 이상)	98	28.0	28.0
	중견기업(100~999명)	126	36.0	64.0
	중소기업(30~99명)	98	28.0	92.0
	스타트업(30명 미만)	28	8.0	100.0
지역	서울/경기	227	64.9	64.9
	부산/대구/대전	78	22.3	87.2
	기타	45	12.8	100.0

3.2. 변수 정의 및 측정 도구

본 연구에서는 네 가지 주요 변수를 측정했다.

첫 번째 변수는 SBOM 역할 인식으로, 4개의 차원과 11개의 구체적 문항으로 구성되었다. SBOM의 역할 인식은 공급망 투명성 역할, 취약점 관리 역할, 라이선스 준수 역할, 사고 대응 역할의 4가지 차원으로 분류되었다. 이러한 다차원적 구성은 SBOM이 단순한 기술 도구를 넘어 조직의 여러 기능 영역에 미치는 영향을 포괄적으로 측정하기 위함이었다.

두 번째 변수는 기술적 준비도(역량)으로, 개발자들이 실제로 SBOM을 구현할 수 있는 능력을 측정했다. 세부 항목으로는 SBOM 도구 사용 경험, 자동화 수준, 보안 관련 기술 숙련도가 포함되었다. 이 변수는 개발자들의 주관적 인식뿐만 아니라 객관적인 기술 역량을 평가하기 위해 설계되었다.

세 번째 변수는 조직 지원 환경으로, 기업 차원에서 제공하는 지원의 수준을 측정했다. 구체적으로는 도구와 소프트웨어 제공, 예산 할당, 개발 시간 배정, 정책과 가이드라인 제공이 포함되었다. 이 변수는 개발자의 역량과 별개로, 조직이 SBOM 도입을 얼마나 지원하는지를 평가하기 위함이었다.

네 번째 변수는 도입 의도 및 행동으로, 개발자들의 향후 12개월 도입 계획과 현재의 도입 상황을 측정했다. 이 변수는 ABG를 규명하는 데 핵심적인 역할을 했다.

해당 연구의 척도 개발 과정은 체계적인 타당성 확보 절차를 통해 진행되었다.

초기 문항 개발 단계에서는 선행 연구(Compeau & Higgins, 1995; Davis, 1989; Venkatesh & Bala, 2008 등)를 기반으로 개념 정의를 수행하고 전문가 협의를 통해 총 45개 문항을 도출하였다. 이후 소프트웨어 보안 분야 전문가 1명, 보안 업계 전문가 2명, 보안 도구 개발자 3명, 대학교수 1명으로 구성된 전문가 패널이 각 문항의 적절성(relevance), 명확성(clarity), 중복성(redundancy)을 4점 Likert 척도로 평가하였으며, 평균 3.0점 이상 및 Content Validity Ratio(CVR) 〉 0.57 기준을 적용하여 41개 문항으로 정제하였다. 파일럿 조사는 n=78명의 개발자(백엔드 30명, 프론트엔드 22명 등)를 대상으로 Naver Forms를 통해 2025년 9월 16일~10월 5일 동안 실시되었으며, 응답률 91.8%를 기록하였다. 신뢰도 검증 결과 모든 변수의 Cronbach's α가 0.876(SBOM 역할 인식 0.892, 기술적 준비도 0.876, 지각된 조직·환경 0.898, 도입 의도 0.891) 이상으로 우수한 내부 일관성을 확인하였고, 항목-전체 상관계수(Item-Total Correlation) 역시 $r > 0.7$ 기준을 충족하였다.

이러한 다단계 검증 과정은 본 연구 척도의 내용 타당성 및 신뢰성을 확보하며, SBOM 도입 의도 연구의 방법론적 엄격성을 입증한다.

모든 변수는 Likert 5점 척도를 사용하여 측정했다. 척도는 1 (전혀 동의하지 않음)부터 5 (매우 동의함)까지로 구성되었다. 이러한 5점 척도는 응답자의 미묘한 의견 차이를 포착할 수 있으면서도 통계 분석에 충분한 정보를 제공한다.

3.3. 데이터 수집 및 분석 방법

수집된 데이터는 다양한 통계 기법을 사용하여 분석했다. 먼저 기술통계로 평균(M), 표준편차(SD), 빈도 분석을 실시했다. 이는 각 변수의 중심 경향과 분산을 파악하기 위한 기초적인 분석이었다. 다음으로 신뢰도 검증을 위해 Cronbach's α 계수를 계산했다. 이를 통해 각 측정도구가 내적 일관성을 가지고 있는지 확인했으며, 일반적으로 0.7 이상을 기준으로 신뢰도가 있다고 판단했다. 아래의 표 2는 각 변수별 Cronbach's α 결과를 보여준다(표 2).

표 2. Cronbach's α를 통한 신뢰도 검증

변수	문항 수	Cronbach's α	평가	기준
SBOM 역할 인식	11	0.892	우수	$\alpha > 0.7$
기술적 준비도	10	0.876	우수	$\alpha > 0.7$
지각된 조직·환경	11	0.898	우수	$\alpha > 0.7$
도입 의도	9	0.891	우수	$\alpha > 0.7$
전체	41	0.908	우수	$\alpha > 0.7$

모든 변수의 α 값이 0.876 이상으로, 내적 일관성이 우수한 수준임을 확인하였다.

핵심적인 분석은 격차 분석이었다. 절대 격차는 두 변수 간의 평균 차이를 직접 계산했고, 상대 %격차는 절대 격차를 기준값으로 나누어 백분율로 표시했다. 예를 들어, SBOM 역할 인식(M = 4.11)과 지각된 조직·환경(M = 2.79)의 절대 격차는 1.32였으며, 상대 % 격차는 (1.32 / 4.11) × 100 = 32.1%로 계산되었다. 주요 변수의 평균과 표준편차는 표 3과 같다.

표 3. 주요 변수 간 평균값 및 표준편차 비교

변수	평균(M)	표준편차	순서	비고
SBOM 역할 인식	4.11	0.92	1위	높음
개인 도입 의도	3.42	1.13	2위	중간
개인 기술적 준비도	2.99	1.21	3위	낮음
지각된 조직·환경	2.79	1.20	4위	가장 낮음
SBOM 학습 투자 의향	3.15	1.24	N/A	개인 도입 의도 세부 항목

격차 분석에서 인식-환경 격차(Awareness-Environment Gap)는 SBOM 역할 인식(4.11점)과 지각된 조직·환경(2.79점) 간 1.32점(32.1% 차이)으로, 개발자들이 SBOM의 중요성을 알지만 조직의 준비가 매우 미흡함을 보여준다.

인식-역량 격차(Awareness-Competency Gap)는 SBOM 역할 인식(4.11점)과 개인 기술적 준비도(2.99점) 간 1.12점(27.2% 차이)으로, 개발자들이 SBOM을 중요하게 여기지만 실행 능력이 심각하게 부족함을 나타낸다.

인식-행동 격차(Awareness-Action Gap)는 SBOM 역할 인식(4.11점)과 실제 도입 행동(3.15점) 간 0.96점(23.4% 차이)으로, 인식 수준에 비해 실제 도입이 충분히 이루어지지 않고 있음을 시사한다.

의도-행동 격차(Intention-Action Gap)는 개인 도입 의도(3.42점)와 학습 투자 의향(3.15점)(현재 도입 행동) 간 0.27점(7.8% 차이)으로, 네 가지 격차 중 가장 작아 명확한 의도와 조직의 요구가 주어질 경우 실제 도입으로 이어질 가능성이 높음을 보여준다.

정책적 시사점에서 이 격차들은 SBOM 도입 전략에 다음과 같은 방향을 제시한다. 교육·훈련 강화로 역량 갭을 메우기 위해 도구 사용, 표준 이해, 자동화 방법론 교육이 필요하며, 조직 정책 수립으로 환경 갭을 메우기 위해 경영진 인식 제고, 도구 투자, 프로세스 통합이 필수이다. 사용성 개선으로 의도-행동 갭을 줄이기 위해 자동화 도구, 원클릭 솔루션, 통합 워크플로우 강화가 요구된다.

4. 연구 결과

4.1. GDPR 규제 실패 사례와 교훈

앞서 분석한 GDPR 과징금 현황(약 56억 5천만 유로)은 다음과 같은 매우 실질적인 교훈들을 제시한다.

4.1.1. 첫 번째 교훈: 과징금 규모의 지수적 증가

GDPR 과징금의 규모 변화를 GDPR Enforcement Tracker 통계를 기준으로 살펴보면, 2018~2019년에는 수십만 유로에서 수천만 유로 수준의 비교적 작은 금액과 적은 건수의 과징금 위주로 집행되며 일종의 'orientation phase'를 보였다. 이후 2020~2021년에 접어들면서 아마존, Meta 등 대형 플랫폼을 대상으로 한 고액 과징금이 부과되기 시작하면서 누적 과징금이 수억 유로에서 수십억 유로대로 급격히 증가하였고, 2023년에는 첫 10억 유로대 단일 과징금이 부과되면서 누적액이 40억 유로를 넘어섰다.

2025년 3월 1일 기준 CMS GDPR Enforcement Tracker Report는 2018년 5월 발효 이후 약 6년 8개월 동안 집계된 누적 과징금이 총 2,245건, 약 56억 5천만 유로에 이른다고 보고하고 있어, 초기 몇 년과 비교할 때 집행 강도가 사실상 지수적으로 강화되었음을 보여준다. 이러한 추세는 규제 당국의 집행 강화가 일시적 캠페인이 아니라 장기적·구조적 변화라는 점을 시사하며, 초기 단계에서 GDPR 규제의 심각성을 과소평가했던 기업일수록 시간이 지날수록 더 큰 재정적 타격을 입게 되었음을 의미한다. 이와 같은 패턴을 고려하면, CRA 역시 시행 초기에는 완만한 집행으로 시작하더라도 일정 시점 이후 집행 강도가 급격히 증가할 가능성이 높으며, 2027년 본격 시행 직전에 준비를 시작하는 기업들은 GDPR 초기 대응에 실패한 기업들과 유사한 위험에 직면할 수 있다.

4.1.2. 두 번째 교훈: 선제적 대응의 중요성

GDPR 발효 전(2015-2017년) 기간에 충분한 준비를 한 기업들과 발효 후에 대응을 시작한 기업들의 과징금 규모를 비교하면 명확한 차이가 드러난다. 발효 전에 준비한 기업들의 경우 평균 과징금이 현저히 낮았으며, 일부는 과징금을 피할 수 있었다. 반면 미 준비 기업들의 경우 규제 당국의 집중 단속 대상이 되어 평균 과징금이 급증했다. 이는 선제적 대응이 단순한 기업의 책임 문제를 넘어 실질적인 비용 절감 효과를 가져온다는 것을 보여준다.

CRA의 맥락에서 보면, 2027년 시행까지의 남은 기간은 선제적 대응의 마지막 기회이다. 2026년 현시점에서 준비를 시작하는 기업들은 충분한 시간을 확보할 수 있지만, 2027년에 준비를 시작하려는 기업들은 심각한 시간 부족에 직면할 것이다.

4.1.3. 세 번째 교훈: 프로세스 정비의 우선성

GDPR 과징금의 50% 이상이 "동의 부족" 관련 위반이라는 점은 매우 중요한 시사점을 제공한다. 이는 기업들이 기술 개선에는 상당한 투자를 했음에도 불구하고, 법적 프로세스 정비에는 상대적으로 미흡했다는 것을 의미한다.

쿠키배너 설치, 개인정보처리방침 작성, 동의 관리 시스템 구축 등의 기본적인 조치들이 여전히 많은 기업에서 미흡했던 것이다. 이는 CRA 대응에도 중요한 교훈을 제공한다. SBOM 생성 도구 도입 같은 기술적 조치도 중요하지만, 조직 내에서 SBOM을 관리하고 취약점에 대응하는 프로세스를 정비하는 것이 더욱 중요하다는 의미이다.

4.2. SBOM ABG 분석

본 연구의 가장 핵심적인 발견은 개발자들의 SBOM에 대한 인식과 실제 행동 간의 격차에 관한 것이다. SBOM 채택과 관련된 ABG를 보다 세분화하여, 인식-환경 격차, 인식-역량 격차, 인식-행동 격차, 의도-행동 격차의 네 가지 하위 격차로 분석 한다. 각 격차는 서로 다른 원인과 해결책을 시사한다.

4.2.1. 첫 번째 격차: 인식-환경 격차 (32.1%)

이 격차는 모든 격차 중에서 가장 심각한 것으로 나타났다. 개발자들의 SBOM 필요성 인식은 높은 수준(M = 4.11)으로, 대부분의 개발자들이 SBOM의 중요성을 충분히 이해하고 있었다. 그러나 조직의 지원 수준은 훨씬 낮았다(M = 2.79). 이는 절대 격차 1.32, 상대 % 격차 32.1%에 해당한다. 이러한 격차가 의미하는 바는 다음과 같다. 개발자들이 SBOM을 도입하지 않는 이유는 그들이 SBOM의 필요성을 모르기 때문이 아니라, 조직에서 충분한 도구, 예산, 시간, 정책적 지원을 제공하지 않기 때문이라는 것이다. 따라서 해결책은 개발자의 의식 제고가 아니라, 조직 차원에서의 투자와 정책 개선이 필요하다는 의미이다.

더 구체적으로 살펴보면, 조직 지원 부족의 세부 내용은 다음과 같다. 먼저 도구 및 소프트웨어 제공 부족으로, 많은 기업들이 SBOM 생성 도구를 보유하지 않고 있었거나, 보유하더라도 개발팀이 접근할 수 없었다. 다음으로 예산 할당 부족으로, SBOM 도구 도입이나 보안 교육에 필요한 예산이 확보되지 않았다. 셋째로 개발 시간 배정 부족으로, 개발자들이 기존 프로젝트에 바쁜 와중에 SBOM 관련 추가 작업을 할 여유가 없었다. 넷째로 정책 및 가이드라인 제공 부족으로, 조직에서 SBOM 도입에 대한 명확한 지시나 기준을 제시하지 않았다.

4.2.2. 두 번째 격차: 인식-역량 격차 (27.2%)

개발자들의 SBOM에 대한 인식(M = 4.11)은 높지만, 실제 구현 역량(M = 2.99)은 현저히 낮았다. 이는 절대 격차 1.12, 상대 % 격차 27.2%에 해당한다. 이러한 격차는 개발자들이 SBOM의 필요성을 충분히 인식하고 있음에도 불구하고, 실제로 SBOM을 생성하고 관리할 수 있는 능력이 부족하다는 것을 의미한다.

역량 부족의 구체적인 원인들은 다음과 같다.

첫 번째로 SBOM 도구 사용 경험 부족으로, 대부분의 개발자들이 SBOM 관련 도구를 사용해본 적이 없었다.

두 번째로는 자동화 수준의 낮음으로, 많은 기업들이 SBOM 생성 과정을 수동으로 진행하고 있었으며, 자동화되지 않은 프로세스는 오류가 많고 시간이 많이 걸린다.

세 번째로 보안 관련 기술 숙련도의 부족으로, SBOM 관리는 단순한 개발 기술뿐만 아니라 보안 지식도 요구하지만, 이에 대한 교육이 부족했다.

해결책은 개발자 교육 및 훈련 프로그램의 강화이다. SBOM 개념과 도구 사용법에 대한 체계적인 교육을 제공함으로써 역량 격차를 줄일 수 있다. 또한 자동화 도구의 도입으로 개발자들의 수작업 부담을 줄이고, 효율성을 높일 수 있다.

4.2.3. 세 번째 격차: 인식-행동 격차 (23.4%)

개발자들의 SBOM에 대한 인식(M = 4.11)과 실제 도입 행동(M = 3.15) 간에도 격차가 존재했다. 이는 절대 격차 0.96, 상대 % 격차 23.4%에 해당한다. 이 격차는 인식-환경 격차나 인식-역량 격차보다는 작지만, 여전히 유의미한 수준이다. 이는 일부 개발자들이 SBOM의 필요성을 인식하고 있음에도 불구하고, 실제로는 SBOM 도입을 진행하지 않고 있다는 것을 의미한다.

인식-행동 격차의 원인은 다양하다. 첫째, 시간 부족으로, SBOM 도입이 추가적인 시간 투자를 요구하기 때문이다. 둘째, 우선순위 낮음으로, 기존 개발 업무에 비해 SBOM을 낮은 우선순위로 인식했다. 셋째, 초기 학습 곡선으로, 새로운 도구와 프로세스를 학습하는 초기 단계에서의 어려움이 있었다. 넷째, 명확한 지시 부족으로, 조직에서 SBOM 도입에 대한 강제적이거나 명확한 지시를 제공하지 않았다.

해결책은 기술 지원 강화와 프로세스 자동화이다. CI/CD 파이프라인에 SBOM 생성 단계를 자동으로 포함시켜, 개발자들이 별도의 추가 작업을 하지 않아도 되도록 할 수 있다. 또한 조직 차원에서 SBOM 도입을 필수 요구사항으로 명시하고, 이를 코드 리뷰나 배포 체크리스트에 포함시킬 수 있다.

4.2.4. 네 번째 격차: 의도-행동 격차 (7.8%)

가장 긍정적인 발견은 의도-행동 격차가 상대적으로 매우 낮다는 점이었다. 개발자들의 향후 12개월 도입 의도(M = 3.42)와 현재 도입 행동(M = 3.15) 간의 차이는 절대 격차 0.27, 상대 %격차 7.8%로, 네 가지 격차 중 가장 작았다. 이는 매우 중요한 시사점을 제공한다.

의도-행동 격차가 작다는 것은 다음을 의미한다. 만약 개발자들이 SBOM 도입에 대한 명확한 의도를 형성하고, 조직이 도입을 명시적으로 요구한다면, 실제 도입 확률이 매우 높다는 것이다. 즉, 문제는 기술적인 실행 불가능성이 아니라, 의사결정 단계의 모호성에 있다는 의미이다. 경영진이 SBOM 도입을 명확하게 지시하고, 조직이 이를 필수 요구사항으로 규정한다면, 개발자들은 이를 충분히 실행할 수 있다는 뜻이다.

4.2.5. 통계적 유의성 검증

격차의 통계적 유의성을 검증하기 위해 대응표본 t-test(paired-samples t-test)를 실시하였다. 각 변수 간 평균 차이가 통계적으로 유의한지 검증하며, 자유도(df = 349), 효과 크기(Cohen's d)[31]도 함께 산출하였다. t-test 결과는 표 4에 제시한다.

표 4. 주요 격차에 대한 대응표본 t-test 결과

격차유형	쌍방 비교 변수	절대 격차 (M 차이)	표준편차 차이 (SD차이)	t(349)	p	Cohen's d*
인식-환경 격차	역할 인식(4.11) vs 조직환경(2.79)	1.32	0.65	20.12	< 0.001	1.05 (대)
인식-역량 격차	역할 인식(4.11) vs 기술준비도(2.99)	1.12	0.61	18.34	< 0.001	0.95 (대)
인식-행동 격차	역할 인식(4.11) vs 도입행동(3.15)	0.96	0.61	15.67	< 0.001	0.85 (대)
의도-행동 격차	도입 의도(3.42) vs 실행행동(3.15)	0.27	0.55	4.89	< 0.001	0.25 (작음)

*0.2=작음, 0.5=중간, 0.8=대

앞서 제시한 네 가지 격차 모두 대응표본 t-test 결과 통계적으로 유의미하였다(표 4). 구체적으로 인식-환경 격차는 $t(349) = 20.12$, $p < 0.001$ (Cohen's $d = 1.05$), 인식-역량 격차는 $t(349) = 18.34$, $p < 0.001$ ($d = 0.95$), 인식-행동 격차는 $t(349) = 15.67$, $p < 0.001$ ($d = 0.85$), 의도-행동 격차는 $t(349) = 4.89$, $p < 0.001$ ($d = 0.25$)로 나타났다. 모든 격차에서 $p < 0.001$ 수준의 강한 통계적 유의성을 보였으며, Cohen's d 값은 인식 관련 격차에서 0.85~1.05로 매우 큰 효과 크기를 보였으나, 의도-행동 격차에서는 0.25로 중간 수준에 머물렀다. 이는 의도-행동 격차가 상대적으로 작지만 조직 정책으로 쉽게 해소 가능함을 시사한다. 이는 각 격차들이 단순한 우연에 의한 것이 아니라, SBOM 도입 과정에서 실제로 존재하는 구조적 문제임을 통계적으로 입증하는 것이다.

4.2.6. 핵심 발견의 종합 해석

이 네 가지 격차의 분석 결과를 종합하면, 다음과 같은 핵심 메시지가 도출된다. 한국의 소프트웨어 개발자들은 SBOM의 중요성을 충분히 인식하고 있으며, 개발 의도도 높은 상태이다. 문제는 조직이 필요한 지원을 제공하지 못하고 있으며, 개발자들이 충분한 역량을 갖추지 못했다는 것이다. 따라서 해결책은 개발자의 의식 제고가 아니라, 조직 차원의 투자와 지원 강화, 그리고 체계적인 교육과 훈련 프로그램의 개발에 있다. CRA 2027년 시행까지 제한된 시간 동안, 한국 기업들이 이러한 조직적 개선을 실현할 수 있느냐가 향후 규제 대응의 성패를 결정할 것이다.

4.3. CRA 대응 단계별 실행 전략

CRA 규제 대응을 성공적으로 이루기 위해서는 구체적이고 실행 가능한 로드맵이 필수적이다. 본 연구에서는 2026년 1분기부터 2027년까지의 기간을 세 개의 단계로 나누어 상세한 실행 전략을 제시하며 방위산업 특화 전략도 같이 제시한다(표 5, 6).

표 5. CRA 대응 단계별 실행 전략

단계	기간	목표	주요 과업
Phase 1 즉시 실행 단계	2026년 1분기 (1~3월)	SBOM 기본 체계 신속 구축, 조직 차원의 방향성과 기반 마련	– SBOM 도입 정책 수립 필수 선언, 책임 부서·담당자 지정, 예산 배정, 단계별 타임라인 설정 – SBOM 도구 평가 및 선정 자동화 수준, CI/CD 통합 가능성, 비용, 지원 언어 등을 기준으로 상용·오픈소스 도구 검토·선정 – 기본 교육 실시 경영진·리더 대상 오리엔테이션, 개발팀 대상 실무 교육(SBOM 개념·도구 사용·취약점 대응 방법) – 파일럿 프로젝트 착수 1~2개 중간 복잡도 기존 프로젝트 선정, 경험 많은 개발자 중심으로 SBOM 생성 적용
Phase 2 단기 확대 단계	2026년 2~3분기 (4~9월)	전사적 SBOM 의무화 및 운영 자동화, 감시 체계 구축	– 전 프로젝트 SBOM 적용 확대 신규·기존 프로젝트로 단계적 확대, 고객 대면·핵심 서비스 우선 적용, 소급 적용 시 인력·시간 배분 계획 수립 – CI/CD 파이프라인 통합 빌드 마지막 단계에 SBOM 자동 생성, 리포지토리 자동 커밋, 배포 전 SBOM 기반 취약점 차단 로직 적용 – 취약점 모니터링 자동화 NVD 등에서 CVE 자동 수집, 내부 SBOM과 매칭, 영향 프로젝트 자동 알림, 48시간 내 영향 평가 체계 구축 – 조직 내 감시 프로그램 운영 월 1회 SBOM 최신성·취약점 대응·라이선스 준수·SBOM 성숙도 점검, 경영진 보고 및 추가 투자·정책 조정 근거로 활용
Phase 3 중기 고도화 단계	2026년 4분기 ~ 2027년	CRA 시행 직전 최종 고도화 및 점검, 외부 공급망·법적 리스크 통합 관리	– 취약점 대응 프로세스 고도화 CVSS 기반 Critical/High/Medium/Low 우선순위 체계 수립, 등급별 대응 시간(예: Critical 24시간, High 1주 등) 규정, 실제 호출 여부 기반 영향도 평가, 패치 테스트 및 안정성 검증 절차 명문화 – 공급업체 SBOM 요구 사용 중인 상용 라이브러리·SaaS 공급업체에 SBOM 요구, 자체 제공 컴포넌트 SBOM 준비, 공급업체 SBOM 기반 라이선스·취약점 검증 체계 구축 – DPA 및 국제 데이터 이전 기준(SCC) 체결 모든 데이터 처리 계약에 DPA 포함, EU→제3국 전송 시 SCC 기반 보호조치 반영, SBOM 수집 과정의 개인정보 처리 법적 근거 점검 – 최종 준비 상태 점검 모든 프로젝트 SBOM 제공 여부, 24/7 취약점 모니터링 가동 여부, 취약점 대응 프로세스 작동성, 공급업체 SBOM 확보 여부, 국제 데이터 이전 계약 정비 여부를 종합 점검하고 미비점 보완

표 6. CRA 대응 단계별 실행 전략(방위산업 특화)

단계	기간	목표	주요 과업
Phase 1 즉시 실행 단계	2026년 1분기 (1~3월)	국방 사업 요구조건과 정합적인 SBOM 기본체계 수립, 군·방사청 요구사항과의 매핑	– 국방 규제·가이드라인 매핑 방위사업청·국방부 보안지침, CMMC/SSDF 등 기존 국방 관련 기준과 CRA·SBOM 요구사항 교차 매핑. – 방산 프로젝트 우선 범위 정의 무기체계·C4I·관제시스템 등 임무 필수 시스템을 1차 SBOM 의무 대상으로 지정. – SBOM 정책 수립(2026년 2월) “국방 사업 수주용 제품/소프트웨어는 2026년 3월 이후 SBOM 필수 제출” 등 방산 입찰·제안요청서(RFP) 반영을 전제로 한 정책 제안. – 도구 선정 시 오프라인/망분리 고려 망분리 환경, 군 시험망 등에서 사용 가능한 SBOM·SCA 도구 검토, 에어갭 배포 가능 여부 평가. – 기본 교육(방산 특화) 방산 PM·체계종합업체 대상 SBOM·공급망 보안 교육, 군 사용자의 보안 요구와의 연계 설명.
Phase 2 단기 확대 단계	2026년 2~3분기 (4~9월)	주요 방산 프로그램 전반으로 SBOM 의무화, 납품·검수 프로세스에 내재화	– 방산 사업별 SBOM 통합 대형 무기체계 프로그램(예: 레이더, 지휘통제체계) 단위로 SBOM을 시스템·서브시스템 수준까지 계층화하여 관리 – CI/CD·형상관리와 연계 군/방산 특성상 완전 자동화가 어려운 경우, 최소한 형상관리(형상 통제 이력)와 SBOM을 연동해 릴리스별 SBOM 스냅샷 보관. – 방산 공급망 계층 반영 1차 협력사(체계업체) 뿐 아니라 2·3차 부품/소프트웨어 공급사에 대해서도 SBOM 제출 요구 조건을 계약서·구매요건에 반영. – 취약점 모니터링 시 임무 영향도 평가 CVE 심각도에 더해 “작전 영향도(임무 중지, 성능 저하, 정보유출 등)” 기준을 추가해 우선순위를 설정. – 국방 검수 절차 연계 군 납품 시, 기능·성능 시험과 함께 SBOM 제출 여부, 취약점 잔존 여부를 검수 체크리스트에 포함.
Phase 3 중기 고도화 단계	2026년 4분기 ~ 2027년	동맹 및 수출을 고려한 방산 SBOM 거버넌스 구축, 동맹국 신뢰 확보	– 동맹·수출 대응 SBOM 패키지 해외 수출용 무기체계에 대해, 수출 대상국이 요구할 수 있는 수준(예: NATO, 미 정부 요구)에 맞춘 SBOM·취약점 관리 보고서 템플릿 마련. – 국방 사이버훈련과 연계 사이버 방어 훈련 시 SBOM을 활용한 위협 시나리오(공급망 공격, 악성 라이브러리 교체 등)를 반영, 실전 대응력 강화. – 장기 수명주기 지원 무기체계의 장기 운용(10~30년)을 고려하여, 버전·모듈 교체 시 SBOM을 갱신하는 수명주기 관리 프로세스 확립. – 국방 규제·표준 제안 방산 업계 협의체를 통해 방위사업청에 SBOM 형식·제출 기준(예: CycloneDX/SPDX 기반) 제안, 국방 분야 SBOM 가이드라인 수립에 참여. – 최종 점검(2027년 6월): 모든 핵심 무기체계/정보체계에 대해 SBOM 보유 여부, 취약점 대응 체계, 협력사 SBOM 제출 실적, 수출 프로젝트 대비 상태를 종합 점검.

표 5는 일반 기업을 위한 CRA 대응 단계별 실행 전략을, 표 6은 방위산업 특화 전략을 정리한 것이다. 특히 Phase 1~3으로 나누어 일정과 주요 과업을 구체화함으로써, 2027년 시행까지의 실질적인 로드맵을 제시한다.

4.3.1. Phase 1: 즉시 실행 단계 (2026년 1분기)

4.3.1.1. 목표와 의미

첫 번째 단계의 목표는 SBOM 기본 체계를 신속하게 구축하는 것이다. 이 단계는 가장 중요한 단계이자 가장 시간이 많이 소요되는 단계이다. 자체적으로 준비가 되지 않은 곳들에서는 현시점에서 즉시 시작하지 않으면, 나머지 기간 내에 충분한 준비를 할 수 없을 것이다.

4.3.1.2. SBOM 정책 수립 (2026년 2월)

경영진 차원에서 먼저 해야 할 일은 SBOM 도입에 대한 명확한 정책을 수립하는 것이다. 이는 단순한 문서 작성이 아니라, 조직의 장기적 규제 대응 전략의 핵심이다. 정책에는 다음 항목들이 반드시 포함되어야 한다. 먼저 SBOM 도입의 필수성에 대한 명확한 선언이 필요하다. "모든 신규 개발 프로젝트는 2026년 3월부터 SBOM을 필수적으로 제공해야 한다" 같은 구체적이고 강력한 선언이 필요하다. 다음으로 책임 부서와 담당자 지정으로, 누가 SBOM 도입을 주도하고 관리할 것인지 명확히 해야 한다. 또한 예산 배정으로, SBOM 도구 구입, 교육, 인력 투자 등에 필요한 예산을 명시해야 한다. 마지막으로 타임라인으로, 각 단계별 완료 일정을 구체적으로 제시해야 한다.

4.3.1.3. SBOM 도구 평가 및 선정 (2026년 2월)

병행하여 개발팀과 보안팀이 중심이 되어 SBOM 도구를 평가하고 선정해야 한다. 이 과정은 단순한 도구 선택이 아니라, 향후 3년간의 조직 운영 방식을 결정하는 중요한 의사결정이다.

도구 평가 시 고려해야 할 항목들은 다양하다. 먼저 자동화 수준으로, 빌드 프로세스에서 자동으로 SBOM을 생성할 수 있는 정도를 평가해야 한다. 이상적으로는 80% 이상의 자동화율을 목표로 해야 한다. 다음으로 CI/CD 통합 가능성으로, 기존 개발 파이프라인과 얼마나 쉽게 통합될 수 있는지 확인해야 한다. 또한 비용 요소로, 초기 도입비, 월간 구독료, 지원 비용 등을 종합적으로 검토해야 한다. 마지막으로 지원 언어로, 회사의 주요 개발 언어(Python, Java, JavaScript 등)를 지원하는지 확인해야 한다.

현재 시장에서 추천할 수 있는 도구들은 다음과 같다. 상용 도구로는 Black Duck (Synopsys), Snyk, JFrog Xray 등이 있으며, 이들은 엔터프라이즈급 기능과 지원을 제공한다. 오픈소스 도구로는 SPDX, CycloneDX, Syft 등이 있으며, 초기 비용이 없으나 지원이 제한적이다. 중소기업의 경우 오픈소스 도구로 시작하여 필요에 따라 상용 도구로 확대하는 방식도 좋은 선택이다.

4.3.1.4. 기본 교육 실시 (2026년 3월)

도구 선정과 병행하여 개발팀 전체를 대상으로 기본 교육을 실시해야 한다. 이 교육은 2가지 수준으로 나누어 진행하는 것이 좋다. 먼저 경영진 및 프로젝트 리더를 대상으로 한 2시간의 오리엔테이션으로, SBOM의 개념, CRA 규제의 의미, 그리고 기업의 대응 방향에 대해 설명한다. 다음으로 개발팀을 대상으로 한 4시간의 실무 교육으로, SBOM 도구의 사용 방법, 실제 프로젝트 적용 방법, 취약점 식별 및 대응 방법을 다룬다.

4.3.1.5. 첫 번째 파일럿 프로젝트 시작 (2026년 3월)

교육과 동시에 1~2개의 파일럿 프로젝트를 선정하여 SBOM 생성을 시작한다. 파일럿 프로젝트는 다음의 기준에 따라 선정하는 것이 좋다. 먼저 핵심도가 높지 않으면서도 복잡도가 중간 정도인 프로젝트를 선택해야 한다. 완전히 새로운 프로젝트보다는 기존 프로젝트에 SBOM을 적용하는 것이 현실적이다. 또한 경험 많은 개발자가 참여하는 프로젝트를 선택하여, 학습 과정에서의 문제 해결이 용이하도록 해야 한다.

4.3.2. Phase 2: 단기 확대 단계 (2026년 2-3분기)

4.3.2.1. 목표와 의미

두 번째 단계의 목표는 파일럿 단계에서 얻은 경험을 바탕으로, 전사적 차원에서 SBOM을 의무화하는 것이다. 이 단계를 성공적으로 추진하면, 2026년 이후의 본격적인 규제 대응 준비가 현저히 수월해질 것이다.

4.3.2.2. 모든 프로젝트에 SBOM 적용 (2026년 6월)

Phase 1에서의 파일럿 경험이 축적되면, 6월부터는 신규 프로젝트는 물론 기존 프로젝트에도 SBOM 적용을 확대해야 한다. 이 과정에서는 단계적 접근이 중요하다. 우선적으로는 고객 대면 제품이나 핵심 기능을 담당하는 프로젝트부터 적용을 시작한다. 그 다음으로는 중요도가 중간인 프로젝트로 확대하고, 마지막으로 내부 도구나 부수적 프로젝트에 적용한다.

이 단계에서 개발팀이 직면할 수 있는 어려움들을 미리 예상하고 대비해야 한다. 첫째, 기존 프로젝트에 SBOM을 소급 적용할 때 많은 시간이 소요될 수 있다. 따라서 업무 시간의 일부를 이 작업에 할당하거나, 임시 인력을 투입해야 한다. 둘째, 개발자들의 저항이 있을 수 있다. 새로운 프로세스는 초기에 개발 속도를 낮출 수 있기 때문이다. 이를 극복하기 위해서는 경영진의 강력한 지지와 함께, 실제로 SBOM 도입으로 인한 효율성 개선 사례들을 공유해야 한다.

4.3.2.3. CI/CD 파이프라인 통합 (2026년 6월)

위 내용과 병행하여 DevOps 팀이 중심이 되어 CI/CD 파이프라인에 SBOM 생성 단계를 자동으로 포함시켜야 한다. 이는 SBOM 관리의 지속성을 보장하는 가장 중요한 조치이다.

구체적으로는 다음과 같이 진행한다. 빌드 프로세스의 마지막 단계에 SBOM 생성 단계를 추가한다. 이를 통해 모든 빌드마다 자동으로 최신 SBOM이 생성된다. 그리고 생성된 SBOM을 버전 관리 시스템에 자동으로 커밋하여 이력을 추적할 수 있도록 한다. 또한 배포 전 단계에서 자동으로 SBOM을 검사하여, 알려진 취약점이 있는 라이브러리가 포함되어 있으면 배포를 일시 중단하도록 설정할 수 있다. 이러한 자동화는 개발자의 추가 업무 부담을 크게 줄여준다.

4.3.2.4. 취약점 모니터링 자동화 (2026년 7월)

보안팀이 중심이 되어 새로운 취약점 정보를 자동으로 모니터링하고, 영향받는 프로젝트를 식별하는 시스템을 구축해야 한다. 현재 시장에는 여러 취약점 모니터링 서비스가 있으며, 이들을 활용할 수 있다.

구체적인 방안은 다음과 같다. 매일 NVD(National Vulnerability Database)와 다른 취약점 정보 소스에서 새로운 CVE를 수집한다. 그리고 기업이 보유한 모든 SBOM과 비교하여, 영향받는

프로젝트를 식별한다. 영향받는 프로젝트가 발견되면 자동으로 관련 팀에 알림을 보낸다. CRA의 요구사항에 따르면 이러한 평가를 48시간 이내에 완료해야 하므로, 신속한 자동화가 필수적이다.

4.3.2.5. 조직 내 감시 프로그램 (2026년 8월)

감시팀이 중심이 되어 조직 전체의 SBOM 준수 현황을 정기적으로 점검하는 프로그램을 시작한다. 이는 Phase 3에서의 최종 준비를 위한 기초 자료를 제공한다.

구체적으로는 월 1회 정도 다음 항목들을 점검한다. 각 프로젝트의 SBOM 제공 여부와 최신 정도, 발견된 취약점의 대응 현황, 라이선스 준수 현황, 그리고 전체 조직의 SBOM 성숙도 지수 등을 평가한다. 이러한 감시 데이터는 경영진 리포팅에 활용되며, 필요한 추가 투자나 정책 조정을 결정하는 데 활용된다.

4.3.3. Phase 3: 중기 고도화 단계 (2026년 4분기 ~ 2027년)

4.3.3.1. 목표와 의미

세 번째 단계의 목표는 CRA 2027년 본격 시행을 앞두고, 모든 준비 사항을 최종 점검하고 미흡한 부분을 고도화하는 것이다. 이 단계에서는 기술적 준비뿐만 아니라, 법적, 조직적 준비도 함께 진행된다.

4.3.3.2. 취약점 대응 프로세스 고도화 (2027년 1분기)

Phase 2에서 구축한 자동 모니터링 시스템을 더욱 정교하게 다듬어, 실제 위험 상황에서도 신속하게 대응할 수 있도록 해야 한다. 취약점 대응 프로세스는 다음과 같이 구성된다.

먼저 우선순위 기준을 명확히 해야 한다. CVSS(Common Vulnerability Scoring System) 점수에 따라 Critical(9.0~10.0), High(7.0~8.9), Medium(4.0~6.9), Low(0.1~3.9)로 분류하고, 각 등급에 따라 서로 다른 대응 시간을 설정한다. 또한 취약점이 실제로 개발한 코드에서 호출되는 함수인지 확인하여, 영향도를 보다 정확히 평가해야 한다. 예를 들어, CVSS 점수가 높더라도 실제로는 사용하지 않는 라이브러리의 취약점이라면, 우선순위를 낮출 수 있다.

다음으로 대응 시간을 규정해야 한다. Critical 취약점은 24시간 이내에 패치를 배포하거나, 최소한 임시 조치(기능 비활성화, 네트워크 차단 등)를 취해야 한다. High 취약점은 1주일 이내에, Medium 취약점은 2주일 이내에 패치를 배포한다. Low 취약점은 정기 업데이트 시에 포함시킨다.

또한 패치 테스트 절차를 명확히 해야 한다. 신속한 대응만큼 중요한 것이 안정성이다. 패치 적용 후 기존 기능이 정상 작동하는지, 새로운 부작용이 없는지 충분히 테스트한 후에야 배포해야 한다. CRA 규제에서는 신속성을 강조하지만, 패치로 인한 새로운 문제를 일으키면 안 된다.

4.3.3.3. 공급업체 SBOM 요구 (2027년 1분기~)

기업이 사용하는 외부 라이브러리나 SaaS 서비스의 제공 업체들에게 SBOM 제공을 요청하기 시작한다. 이는 간접 의존성 관리의 첫 번째 단계이다.

공급업체 관리 전략은 다음과 같다. 먼저 기업이 사용 중인 주요 상용 라이브러리 제공 업체(예: Spring Framework, React 등)에게 SBOM 제공을 요청한다. 대부분의 평판 있는 오픈소스 프로젝트들은 이미 SBOM을 제공하고 있거나 이를 추진 중이다. 다음으로 자체 개발한 컴포넌트를 다

른 팀이나 외부에 제공하는 경우, 이에 대한 SBOM도 준비해야 한다. 마지막으로 공급업체의 SBOM을 수집한 후, 라이선스 컴플라이언스를 검증하고, 알려진 취약점이 없는지 확인한다.

4.3.3.4. DPA 및 국제 데이터 이전 기준(SCC) 체결 (2027년 2분기 내)

법무팀이 중심이 되어 국제 데이터 처리 관련 계약과 규제를 정비한다. GDPR 사례에서 보았듯이, 국제 데이터 이전이 가장 심각한 위반 사항 중 하나이므로, 미리 대비해야 한다.

구체적으로는 다음과 같다. 먼저 DPA(Data Processing Agreement)를 모든 데이터 처리 계약에 포함시켜, 개인정보 처리의 법적 근거를 명확히 한다. 다음으로 EU에서 미국 또는 다른 국가로의 데이터 이전이 있는 경우, SCC(Standard Contractual Clauses)에 따라 적절한 보안 조치를 취한다. SBOM 수집 과정에서 사용자의 개인정보가 처리된다면, 이러한 법적 체크가 필수적이다.

4.3.3.5. 최종 준비 상태 점검 (2027년 6월)

CRA 본격 시행 6개월 전인 2027년 6월, 경영층이 중심이 되어 조직의 최종 준비 현황을 점검한다. 이 시점에서 모든 준비가 완료되지 않으면, 규제 시행 시점에 심각한 문제에 직면할 것이다.

최종 점검의 핵심 항목들은 다음과 같다. 모든 프로젝트에 SBOM이 제공되는가? 취약점 모니터링 시스템이 24/7 정상 작동하는가? 발견된 취약점에 대한 대응 프로세스가 제때 작동하는가? 공급업체로부터 필요한 SBOM을 모두 수집했는가? 국제 데이터 이전 관련 법적 계약들이 모두 체결되었는가? 이 모든 항목에서 긍정적인 답변이 나올 때까지, 지속적인 개선을 진행해야 한다.

5. 논의

5.1. 기업 차원의 전략: “규제는 비용이 아니라 투자”

GDPR 사례에서 명확하게 보았듯이, 규제에 대한 선제적 대응은 기업에게 여러 가지 실질적인 이득을 가져온다. 첫 번째 이득은 과징금 회피이다. GDPR 발효 이전에 충분히 준비한 기업들은 규제 당국의 엄격한 감시 대상에서 벗어날 수 있었다. 규제 당국은 이미 준수하고 있는 기업들을 집중적으로 조사하기보다는, 준수하지 않는 기업들을 찾아내는 데 자원을 집중한다. 따라서 현 시점에서 SBOM 준수를 선제적으로 시작하면, 2027년 이후 규제 집행 시점에 규제 당국의 조사 대상이 될 가능성을 크게 낮출 수 있다.

두 번째 이득은 시장 진출 우위이다. CRA 준수가 EU 시장 진출의 필수 조건이 될 것이라는 점은 이미 명확하다. 현재 준비하고 있는 기업들이 2027년 이후 EU 시장에 진출할 때, 규제 준수를 위한 긴급 대응으로 인한 비용과 시간 낭비를 피할 수 있다. 반면 준비하지 않은 기업들은 규제 시행 이후에 급히 대응하느라 시간과 비용이 소요될 것이고, 이로 인해 시장 진출이 지연될 수 있다.

세 번째 이득은 기업 평판 관리이다. 보안 선진기업으로서의 이미지는 고객 신뢰도에 직접 영향을 미친다. 특히 방위산업이나 금융 산업 같은 보안이 중요한 분야에서는 더욱 그렇다. SBOM을 적극적으로 관리하고 있는 기업은 “보안에 진지하게 대응하는 기업”으로 인식될 것이고, 이는 영업 경쟁력으로 직결된다.

이러한 이득들을 고려할 때, CRA 대응을 위한 투자는 단순한 규제 대응 비용이 아니라, 기업의 장기적 경쟁력을 높이기 위한 전략적 투자로 보아야 한다. 실제로 GDPR에 선제적으로 대응한 많은 EU 기업들이 현재 보안 표준 수립 면에서 선도적 위치에 있으며, 이것이 국제적 신뢰도로 연결

되고 있다.

5.2. 정부 정책 차원의 함의

현재 한국 정부는 소프트웨어 공급망 보안에 대해 아직 구체적인 정책을 제시하지 않고 있다. 그러나 국제적 규제 추세와 국내 산업의 국제 경쟁력을 고려할 때, 정부의 선제적 정책 마련이 필수적이다.

5.2.1. 첫 번째 정책 제안: 국내 SBOM 의무화 로드맵 수립

한국 정부는 CRA에 명시된 것처럼 2027년 또는 2028년부터 국내 디지털 제품에 대한 SBOM 의무화를 추진해야 한다. 이는 여러 가지 이유에서 중요하다. 첫째, 국방·보안 산업의 공급망 투명성을 확보함으로써 국가 안보를 강화할 수 있다. 둘째, 국내 소프트웨어 기업들의 국제 경쟁력을 높일 수 있다. 현재 국내 기업들이 EU 시장 진출 시 CRA 준수를 요구받으므로, 정부가 이미 국내에서 SBOM 의무화를 추진하고 있다면, 국내 기업들의 대응이 훨씬 수월할 것이다. 셋째, 규제 예측 가능성을 제공함으로써 기업들의 전략적 대응을 가능하게 할 수 있다.

구체적으로 정부는 다음과 같은 로드맵을 수립하고 공개해야 한다. 2026년 중에는 SBOM 의무화에 대한 기본 방향과 예상 규제 내용을 공개한다. 2026년에는 법안을 마련하고 산업계의 의견을 수렴한다. 2027년부터는 단계적으로 의무화를 시작한다. 초기에는 정부 조달 소프트웨어부터 시작하고, 점차 방위산업, 금융, 의료 등 핵심 산업으로 확대한다.

5.2.2. 두 번째 정책 제안: SBOM 도구 국산화 및 지원

현재 시장의 주요 SBOM 도구들은 대부분 해외 기업이 개발한 것이거나 오픈소스이다. 한국의 소프트웨어 산업을 강화하기 위해서는 국산 SBOM 도구 개발을 지원해야 한다. 이는 단순한 기술 개발 문제를 넘어, 국내 소프트웨어 산업 생태계를 구축하는 의미가 있다.

구체적으로는 다음과 같은 지원책이 필요하다. 정보통신산업진흥원이나 소프트웨어정책연구소 같은 정부 기관이 중심이 되어, 국산 SBOM 도구 개발 R&D에 연 100억 원 규모의 지원을 실시한다. 또한 중소기업들이 SBOM 도구를 도입할 때, 구매비의 50%를 지원하는 보조금 프로그램을 운영한다. 이를 통해 국산 도구의 시장 점유율을 높일 수 있을 것이다.

5.2.3. 세 번째 정책 제안: 개발자 교육 및 자격화

SBOM 채택의 핵심은 개발자들의 역량이다. 현재 한국의 대학 소프트웨어 교육에서는 SBOM이나 소프트웨어 공급망 보안이 거의 다루어지지 않고 있다. 이를 개선하기 위해서는 정부의 적극적인 개입이 필요하다.

구체적으로는 다음과 같은 조치가 필요하다. 교육부는 대학의 소프트웨어학과 표준 커리큘럼에 "소프트웨어 공급망 보안" 과목을 필수 과목으로 추가하도록 권고한다. 한국 소프트웨어진흥원이 중심이 되어 "SBOM 전문가 자격과정"을 개발하고, 이를 전국의 교육 기관에서 제공하도록 한다. 또한 기업에서 근무하는 개발자들을 위한 온라인 교육 프로그램을 정부 예산으로 무료 또는 저가로 제공한다.

5.2.4. 네 번째 정책 제안: 방위사업청 규제 정비

국방 산업은 보안이 가장 중요한 산업이다. 현재 방위사업청은 방산 기업들에 대해 정보보안 규제를 강화하고 있으나, SBOM 관련 구체적인 요구사항은 아직 제시하지 않고 있다. 이를 개선해야 한다.

구체적으로는 다음과 같은 조치가 필요하다. 방위사업청은 2026년 중에 "방위사업 SBOM 의무화 계획"을 발표하고, 2026년부터 단계적으로 적용한다. 방위사업법을 개정하여 SBOM 요구조건을 명시한다. 또한 방위사업 협회와 함께 SBOM 작성 가이드라인을 개발하여 방산 기업들이 실제로 참고할 수 있도록 한다.

5.3. 개발자 역량 강화 전략

본 연구에서 나타난 가장 큰 격차 중 하나가 역량 격차(27.2%)였다. 이를 해소하기 위해서는 체계적인 개발자 교육 프로그램이 필수적이다.

개발자 차원의 자기계발 경로는 3단계로 나누어 제시할 수 있다. 1단계(2026년 상반기): SBOM 기초 개념 및 도구 학습에서는, 개발자들이 SBOM이 무엇인지, 왜 필요한지, 그리고 주요 도구들이 어떻게 작동하는지를 이해해야 한다. 추천되는 학습 방법은 온라인 과정을 활용하는 것이다. Coursera, Udemy, Linux Academy 등에서 SPDX와 CycloneDX에 대한 기본 과정을 찾을 수 있으며, 대략 20-30시간의 학습이 필요하다. 또한 GitHub의 오픈소스 SBOM 프로젝트들을 직접 살펴보면서 실제 SBOM이 어떻게 구성되어 있는지 이해할 수 있다.

2단계(2026년 하반기): SBOM 생성 및 검증 실무에서는, 개발자들이 실제 프로젝트에서 SBOM을 생성하고 검증하는 경험을 쌓는다. 이상적으로는 조직 내 파일럿 프로젝트에 참여하여, 실제 SBOM 생성 도구를 사용해보고, CI/CD 파이프라인에 통합해본다. 또한 발견된 취약점에 대해 실제로 어떻게 우선순위를 정하고 대응하는지를 배운다. 이 단계에는 약 40-50시간의 실무 학습이 필요하며, 온라인 과정보다는 실제 프로젝트 참여와 팀의 멘토링이 더 효과적이다.

3단계(2027년 이후): SBOM 아키텍처 및 전략 설계에서는, 경험을 쌓은 개발자들이 조직 내에서 SBOM 관련 리더 역할을 수행하게 된다. 예를 들어, 새로운 팀원들을 교육하고, 조직의 SBOM 정책을 수립하며, 공급업체 관리를 주도한다. 이러한 역할을 수행하려면 SBOM뿐만 아니라 소프트웨어 공급망 보안 전체에 대한 깊이 있는 이해가 필요하다.

이러한 개발자 역량 강화 전략이 효과적으로 작동하려면, 조직의 지원이 필수적이다. 경영진이 개발자의 학습과 자기계발을 적극 지원하고, 이를 평가 항목에 포함시킬 필요가 있다.

5.4. 한국의 전략적 이점과 과제

한국의 소프트웨어 산업은 CRA 대응에서 여러 가지 전략적 이점을 가지고 있다. 동시에 극복해야 할 과제도 있다.

5.4.1. 전략적 이점

첫째, "추격자 이점(Latecomer Advantage)"이다. GDPR이나 미국의 Executive Order 14028은 이미 시행되었거나 진행 중이므로, 한국의 기업들과 정부는 이들의 경험으로부터 배울 수 있다. 즉, 이미 증명된 모범 사례들을 채택하면 되므로, 처음부터 새로운 시스템을 구축하는 EU나 미국 기업들보다 더 효율적으로 대응할 수 있다. 특히 미국 국방부(DoD)는 CMMC 2.0 최종 규

칙을 통해 2025년 11월 10일부터 방위산업 공급망 전반에 대한 사이버보안 인증을 단계적으로 의무화하고 있으며, EO 14028 및 OMB M-22-18에 근거해 SBOM을 연방 소프트웨어 조달과 공급망 위험 관리의 핵심 도구로 활용하도록 요구하고 있다. 한편, DoD는 SWFT(Software Fast Track) 프로그램을 통해 기존 RMF 기반 ATO 절차를 자동화·가속하는 시범 사업을 추진 중이며, CMMC와 SBOM을 포함한 공급망 보안 요구사항을 이 새로운 승인 모델에 통합하려는 전략을 제시하고 있다[26-28]. 표 7은 CMMC 2.0의 레벨 구조와 SBOM 관련 요구사항을 요약한 것이다.

표 7. CMMC2.0 에서의 SBOM 요구

수준	요구사항	SBOM 요구	평가 주체
Level 1	14가지 기본 제어 (NIST SP 800-171 기본)	권장	자체 평가
Level 2	110가지 제어 (NIST SP 800-171 전체)	의무	C3PAO
Level 3	24가지 고급 제어 (NIST SP 800-172)	필수	DIBCAC

그리고 NIST SP 800-37 Rev. 2의 RMF(Risk Management Framework) 7단계에서 SBOM은 공급망 위험 관리(SCRM)의 핵심 입력으로 활용되며, DoD CIO 지침(2025. 7)에서 CMMC·SSDF와 연계를 강조한다. SBOM은 소프트웨어 재고 가시성을 제공해 지속적 모니터링을 지원한다. 아래 표 8은 RMF 7단계별 SBOM 상세적용을 정리한 표이다[29,30].

표 8. RMF 7단계별 SBOM 상세 적용

RMF 단계	주요목적	SBOM 활용	구체적 활동 및 도구
1. 준비 (Prepare)	RMF 실행 준비, 우선순위 설정	소프트웨어 재고·SCRM 계획 수립	SBOM 생성으로 구성요소 목록화, 공급업체 위험 평가 시작
2. 분류 (Categorize)	시스템 분류 및 위험 식별	공급망 입력으로 재고·위험 식별	SBOM 분석으로 CUI/CDI 영향 컴포넌트 식별, FIPS 199 분류 지원
3. 선택 (Select)	보안 통제 선택	VEX 와 연계 우선순위화	SBOM 기반 CVE 매핑, NIST 800-53 통제(예: SA-10 공급망 보호) 선택
4. 구현 (Implement)	통제 배포 및 문서화	SBOM 자동화 도입	CI/CD 에 SBOM 생성 도구(Sonatype 등) 통합, 시스템 보안 계획(SSP)에 SBOM 첨부
5. 평가 (Assess)	통제 효과성 검증	SBOM 정확성 감사	3PAO가 SBOM 검증, 취약점 일치 확인, eMASS 업로드 증거
6. 승인 (Authorize)	ATO 결정	SBOM 으로 잔여 위험 평가	eMASS에 SBOM/VEX 제출, AO(Authorizing Official)가 공급망 위험 수용 결정(SWFT 가속화)
7. 모니터링 (Monitor)	지속적 위험 감시	실시간 SBOM 업데이트	연속 모니터링 도구로 SBOM 변화 감지, 재평가 트리거, cATO(continuous ATO) 지원

위와 같이 이미 구축 진행 중인 사례들을 분석하여 국내에 맞게 도입을 진행할 필요가 있다.

둘째, 방위산업 경쟁력 강화이다. 국방 산업에서 소프트웨어 공급망 보안의 중요성이 갈수록 높아지고 있다. 한국이 선제적으로 SBOM 관련 규제와 기술을 도입한다면, 국방 산업에서 국제적 신뢰도를 높일 수 있으며, 이는 국방 수출에도 긍정적 영향을 미칠 수 있다.

셋째, 소프트웨어 산업의 고도화이다. SBOM 도입은 소프트웨어 개발 프로세스 전체를 체계화하고 고도화하는 계기가 될 수 있다. 이를 통해 한국의 소프트웨어 산업 자체가 한 단계 발전할 수 있을 것이다.

5.4.2. 극복해야 할 과제

첫째, 정부 정책의 명확성 부족이다. 현재 한국 정부는 SBOM 관련 명확한 정책을 제시하지 않고 있으므로, 기업들이 불확실성 속에서 대응해야 한다. 빠른 시일 내에 정부의 명확한 정책 방향이 제시될 필요가 있다.

둘째, 개발자 인력 양성의 지연이다. SBOM 관련 전문 인력이 부족하다. 대학 교육에서도 거의 다루어지지 않았으므로, 즉시 인력 양성 프로그램을 시작해야 한다.

셋째, 중소기업 준비도의 저조이다. 본 연구에서 나타났듯이, 개발자들의 인식은 높지만 조직의 지원이 부족하다. 특히 중소기업들은 SBOM 도입을 위한 투자 여력이 없을 수 있으므로, 정부의 적극적인 재정 지원이 필요하다.

6. 결론

6.1. 주요 결과 종합 요약

본 연구를 통해 도출된 가장 중요한 발견들을 종합하면 다음과 같다.

첫 번째 발견: GDPR 과징금의 지수적 증가 추세

GDPR Enforcement Tracker 통계에 따르면, 2018~2019년 초기에는 수십만~수천만 유로 수준의 소규모 과징금 위주로 집행되던 것이 2020~2021년 대형 플랫폼 대상 고액 과징금 부과 이후 급격히 가속화되었으며, 2023년 첫 10억 유로대 단일 과징금 발생과 함께 누적액이 40억 유로를 돌파했다. 2025년 3월 기준 CMS GDPR Enforcement Tracker Report는 발효 후 6년 8개월간 총 2,245건, 약 56억 5천만 유로의 누적 과징금을 보고하고 있어 초기 집행 수준과 비교할 때 사실상 지수적 증가 양상을 보였다. 이러한 장기적 집행 강도 증가는 CRA 역시 시행 초기 완만한 단계 이후 급격한 집행 강화로 전환될 가능성을 강력히 시사하며, 현 시점(2026년)에서 선제적 대응을 하지 않는 기업들은 2027년 이후 규제 당국의 집중 감시와 막대한 과징금 위험에 직면할 가능성이 매우 높다.

두 번째 발견: 조직 지원 부족이 가장 심각한 장애 요인

개발자들의 SBOM 필요성 인식(M = 4.11)과 조직의 지원 수준(M = 2.79) 간의 격차가 32.1%로, 네 가지 격차 중 가장 심각했다. 이는 문제의 원인이 개발자의 의식 부족이 아니라 조직 차원의 투자와 지원 부족에 있다는 점을 명확히 보여준다. 따라서 해결책도 개발자 교육이 아니라, 조직이 필요한 도구, 예산, 정책적 지원을 제공하는 것에 있다.

세 번째 발견: 의도-행동 격차의 낮음

의도-행동 격차가 7.8%로 매우 낮다는 발견은 매우 긍정적인 신호이다. 이는 조직이 명확한 의도를 표현하고 SBOM 도입을 필수 요구사항으로 규정한다면, 개발자들이 이를 충분히 실행할 수 있다는 의미이다. 즉, 기술적 실행 가능성에는 문제가 없으며, 중요한 것은 경영진의 결단과 조직의 정책이라는 뜻이다.

6.2. 정책적 시사점과 국방·보안 산업 중심의 제안

이 연구 결과는 정부와 기업 모두에게 구체적인 정책적 시사점을 제공한다.

첫 번째로, 방위사업청은 방산기업의 SBOM 의무화 계획을 2026년 중에 수립하고, 2026년부터 단계적으로 도입해야 한다. 국방 산업의 소프트웨어 공급망 투명성 확보는 국가 안보의 핵심이기 때문이다.

두 번째로, 정보통신산업진흥원은 SBOM 도구의 국산화를 위한 R&D 프로젝트를 즉시 시작해야 한다. 현재 시장의 주요 도구들이 해외 기업 제품이므로, 이들에 대한 의존도를 줄이고 국내 기술을 발전시키는 것이 중요하다.

세 번째로, 교육부와 소프트웨어정책연구소는 대학 교육 과정에 소프트웨어 공급망 보안을 포함시켜야 한다. 현재의 교육 체계로는 향후 필요한 전문 인력을 양성할 수 없다.

6.3. 기업의 실무 조언: “2026년은 SBOM 준비의 마지막 황금기”

CRA 규제 시행까지 시간이 얼마 남지 않았다. 본격 시행되기 전 대비할 시간은 매우 짧으면서도 충분한 시간이다. 충분한 시간인 이유는, 지금부터 집중적으로 준비한다면 2027년까지 완벽한 준비를 마칠 수 있기 때문이다. 하지만 짧은 시간인 이유는, 다른 기업들도 같은 시간 내에 준비를 해야 하기 때문에, 지금 바로 준비하지 않으면 나중에 곤란한 상황에 처할 수 있기 때문이다.

따라서 기업의 경영진들에게 전하는 메시지는 명확하다. 현재의 투자는 미래의 위기 회피이자, 국제 경쟁력 강화의 기회라는 점이다. GDPR 사례를 보면, 조기 준비한 기업들이 규제 환경 변화에서 피해를 최소화하고 오히려 경쟁 우위를 확보했다. CRA도 마찬가지가 될 것이다.

6.4. 즉시 실행 체크리스트

구체적으로 기업이 2026년 1분기에 즉시 실행해야 할 사항들은 다음과 같다.

첫 번째로 경영진 결정으로 SBOM 도입 정책을 공식 선언하고, 담당 부서를 지정하며, 예산을 배정해야 한다. 동시에 3개 이상의 SBOM 도구를 평가하여 선택 기준을 마련해야 한다.

두 번째로는 선택된 도구를 도입하고, 전사 차원의 기본 교육을 실시해야 한다. 또한 1-2개의 파일럿 프로젝트를 선정하여 SBOM 생성을 시작해야 한다.

세 번째로 파일럿 프로젝트의 진행 현황을 모니터링하고, 발생하는 문제들을 해결하는 프로세스를 수립해야 한다. 동시에 6월부터의 전사 적용을 준비하기 위해 추가 교육을 실시해야 한다.

이 체크리스트를 모두 완료한 기업들은 2026년 말까지의 Phase 2를 무리 없이 진행할 수 있을 것이고, 2027년 규제 시행 시점에 충분한 준비 상태를 갖출 수 있을 것이다.

6.5. 향후 연구 방향

본 연구를 통해 한국의 소프트웨어 개발자들의 SBOM ABG를 규명했으나, 목적적·눈덩이 표본 추출을 통해 GitHub, 개발자 커뮤니티 등 온라인 플랫폼 중심으로 표본을 모집하였기 때문에, 전체 한국 개발자 집단을 완전하게 대표한다고 보기 어렵다. 또한 방산 업체 종사자 비율이 제한적이어서, 방위산업 특화 결론은 탐색적 의미가 강하며 일반화에 주의가 필요하며, 이러한 한계를 보완하기 위해 향후 연구에서는 확률표본 기반 설계와 방산 종사자 대상을 확대한 조사 설계가 요구되며 향후 더욱 심화된 연구가 필요한 분야들이 있다.

첫째, 산업별 세부 분석으로, 금융, 의료, 방위산업 등 서로 다른 규제 환경에 있는 산업들 간의 SBOM 준비도 차이를 분석하는 연구가 필요하다.

둘째, 국제 비교 연구로, 한국과 다른 국가(일본, 싱가포르, 인도 등)의 SBOM 준비도를 비교하여, 한국의 상대적 위치를 파악하는 연구가 필요하다.

셋째, 정량적 ROI 분석으로, SBOM 도입에 필요한 투자비용과 그로 인한 실제 이득(과징금 회피, 시장 접근성 증대, 운영 효율성 개선 등)을 정량적으로 분석하는 연구가 필요하다.

참고문헌

[1] National Institutes of Standards and Technology (NIST). Cybersecurity and Infrastructure Security Agency (CISA) Software Supply Chain Best Practices. 2021.

[2] FireEye. SolarWinds Supply Chain Compromise. 2020.

[3] National Vulnerability Database (NVD). CVE-2021-44228: Apache Log4j Remote Code Execution. 2021.

[4] Executive Office of the President of the United States. Executive Order 14028: Improving the Nation's Cybersecurity. 2021.

[5] European Commission. Regulation (EU) 2024/2847: Cyber Resilience Act. 2024.

[6] Synopsys. 2024 Open Source Composition Analysis Report: Average open source components in commercial applications. 2024.

[7] Lee, T. GDPR Enforcement Tracker Statistics. https://www.enforcementtracker.com (검색일 2025.12.09).

[8] CMS Law. GDPR Enforcement Tracker Report: Numbers and Figures. 2025.

[9] Kim S, Park J. Korean Software Companies' Readiness for EU CRA Compliance. Journal of Korean Cybersecurity, Vol. 45, No. 3, pp. 234-251. 2024.

[10] Ministry of Defense, Republic of Korea. Defense Industry Supply Chain Transparency Requirements. 2024.

[11] Bygrave, L. A. Data Privacy Law: An International Perspective. Oxford University Press. 2017.

[12] Ajzen, I. The Theory of Planned Behavior. Organizational Behavior and Human Decision Processes, Vol. 50, No. 2, pp.179-211. 1991.

[13] Porter, M. E. On Competition. Harvard Business School Press. 2008.

[14] Regulation (EU) 2016/679. General Data Protection Regulation (GDPR). 2018.

[15] Osano GDPR Fines Tracker. (2025). Historical GDPR Fine Statistics. https://www.osano.com/search?term=Gdpr%20Fines%20Tracker (검색일 2025.12.19).

[16] European Data Protection Board (EDPB). Analysis of Major GDPR Violations: Thematic Report. Brussels: EDPB Publications. 2024.

[17] Korff D. Lessons from GDPR Enforcement: Patterns and Trends. Data Protection & Privacy, Vol. 12, No. 1, pp. 45-67. 2022.

[18] National Telecommunications and Information Administration. Software Bill of Materials (SBOM): Formats and Standards Survey. 2023.

[19] Bohn R. B et al. Supply Chain Risk Management: An Analysis of Best Practices. National Institute of Standards and Technology Special Publication 800-53. 2020.

[20] Perforce Software. State of Software Composition Analysis: 2024 Global Report. San Francisco, CA: Perforce Software Inc. 2024.

[21] GitHub. 2024 Software Supply Chain Security Report. 2024.

[22] Chen A et al. Log4Shell: An Analysis of CVE-2021-44228. IEEE Security & Privacy, Vol. 20, No. 2, pp. 42-53. 2022.

[23] Rashid, A. The Critical Role of SBOM in Preventing Supply Chain Attacks. Communications

of the ACM, Vol. 65, No. 3, pp. 36-41. 2022.

[24] European Commission. Cyber Resilience Act: Reporting Obligations (Articles 14-16). Digital Strategy. https://digital-strategy.ec.europa.eu/en/policies/cra-reporting (검색일 2026. 2. 19.).

[25] ENISA. European Union Agency for Cybersecurity. CRA Vulnerability Reporting Guidelines. https://www.enisa.europa.eu/topics/cyber-resilience-act (검색일 2026. 2. 19).

[26] U.S. Department of Defense. Cybersecurity Maturity Model Certification (CMMC) 2.0 – Details and key resources. Office of the Under Secretary of Defense for Acquisition & Sustainment. 2025.

[27] FOSSA. The Comprehensive Guide to SBOM Compliance Requirements. FOSSA Inc. 2025.

[28] DefenseScoop. New Pentagon Program to Speed Up Software Acquisition and Authorization (SWFT – Software Fast Track ATO). 2025.

[29] Department of Defense CIO. DoD Enterprise DevSecOps Fundamentals v2.5. 2025.

[30] Sonatype. Risk Management Framework and the Sonatype Platform. 2025.

[31] Cohen, J. Statistical Power Analysis for the Behavioral Sciences (2nd ed.). Lawrence Erlbaum Associates. 1988.