사이버안보연구, 1집 2호 2024 가을, 271-304

디지털 공급망 보안 위험과 관리체계 시사점 :

미국 EO-14028의 SW 조달 개선 흐름 연구

0102-271304

최윤성 | 고려대학교

논문접수일 2024년 8월 30일 | 논문심사일 2024년 9월 20일 | 게재확정일 2024년 10월 11일

논문 요약

오늘날 공급망 사이버보안은 경제 및 국가안보와 맥락이 닿아있다. 강대국 간의 경쟁과 지정학적 긴장은 공급망 환경을 더욱 복잡하게 만들고 있으며, 이것은 어느 한 국가가 나서서 해결할 수 없는 글로벌 이슈이다.

공급망 사이버보안 정책의 광범위한 동향을 살펴보는 본 연구는 2021년 바이든 정부의 행정명령(EO-14028)과 백악관 관리예산처의 각서(M-22-18)에서 제시한 '안전한 SW 개발 관행을 통한 SW 공급망 보안 강화' 활동의 이행 흐름에 초점을 맞추고 있다.

격변기 주요국의 정책 동향 연구를 수행하는 이유는 우리에게 유리한 정책과 기술을 도입할 수 있는 최적의 시기를 찾고, 특히 EO-14028을 중심으로 빠르게 진화하는 사이버보안 규제와 제도를 우리나라에 어떻게 적용할 수 있을지 검토하기 위함이다.

본 고는 미국의 다양한 최신 전략, 정책, 법적 프레임워크, 가이드라인을 분석한다. 특히 글로벌 공급망 사이버보안 사고 사례를 통해 국내 SW 공급망 위험관리 체계에 필요한 실무 지식의 기반을 구축하고, 기본 정책 계획 수립을 위한 아이디어를 제시한다.

주제어 디지털 공급망, 경제안보, 위험관리, 자가 증명, SBOM

Ⅰ. 머리말

최근 크라우드스트라이크(CrowdStrike)에서 발생한 보안 소프트웨어(SW) 업데이트 사고는 우리가 매일 의존하는 디지털 인프라의 안정성(Stability)이 얼마나 중요한지 상기시켰다. 디지털 인프라와 이를 구동하는 SW는 네트워크, 시스템, 애플리케이션 등으로 매우 복잡하게 구성되어 있으며, 또한 디지털 공급망(이하 공급망)에 의해 운영되고 있다.

이러한 공급망의 복잡성을 공통 기술로 해소하고 가시성을 높이는 목적으로 미국, EU, 일본 등 주요국에서 제도화가 추진되는 것이 '에스-봄(Software Bill of Materials, SBOM)'이다. SBOM은 'SW 자재 명세서'[1]를 뜻하며, 〈그림 1〉과 같이 여러 공급망에서 SW 부품 정보를 투명하게 공유하는 도구이자 인프라이다. SBOM 공유를 통해 구축된 공급망 신뢰성은 향후 인공지능 ML-BOM이나 클라우드 SaaS-BOM으로 확장될 수 있으며, 서로 다른 디지털 시스템 간의 연결고리 역할을 하여 미래 복원력(Resilience)의 기반이 된다.

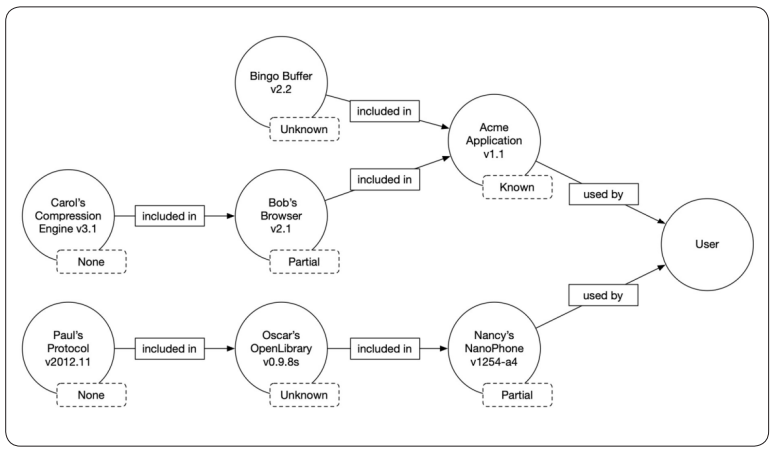
또한 미국에서 올해부터 새롭게 시행된 조달 개선 정책인 '자가 증명(Self-attestation)' 제도가 있다. 자가 증명은 공급망 초기부터 안전한 SW 개발을 보장하기 위해 제조사와 책임을 공유하는 것으로, 미국

1) 미국은 SBOM을 'SW 재료의 목록'이며 "SW 구축에 사용되는 다양한 구성요소의 세부 사항과 공급망 관계를 포함하는 공식적인 기록"으로 정의 [NTIA]

연방기관의 조달 규정과 관련 법률을 연계하여 SW 생태계의 안전하고 신뢰할 수 있는 공급자를 식별하는 데 도움을 준다.

그동안 발생한 공급망 취약성과 사이버공격은 이제 디지털 혁신과 손쉬운 상호 연결을 통해 구축한 기반을 더욱 공고히 해야 하며, 이러한 디지털 인프라가 우리 기업의 경쟁력뿐만 아니라 국가 경제 안보에도 중요하다는 사실을 일깨운다.

〈그림 1〉 두 개의 SW 공급망이 표현된 SBOM 그래프 예시



출처 : Framing Software Component Transparency (CISA, 2024.09)

Ⅱ. 디지털 공급망과 사이버보안

1. 공급망 사이버공격의 위험성

2020년 3월에 발생한 솔라윈즈(SolarWinds) 사건은 공급망 사이버 공격의 대표적인 사례이다. 이 공격은 IT 소프트웨어 공급업체의 배포 시스템에 악성코드를 설치하는 방식으로 30만 명의 고객 중 1만 8천개 회사가 피해를 보았으며 국토안보부, 국무부, 상무부, 재무부를 포함한 9개 미국 연방 부처에 영향을 미쳤다. 이후 2021년 9월, 솔라윈즈는 정보 유출로 인해 4천만 달러의 손실이 발생했다고 공개했으며, 언론은 고객 복구 비용에만 1천억 달러가 넘을 것으로 추정했다(Gopal 2021).

2021년 세계 최대 방산업체 중 하나인 록히드마틴(Lockheed Martin) 데이터 센터가 글로벌 보안 기업 RSA의 SecureID 제품을 통해 해킹당했다는 기사[2]가 와이어드(WIRED)에 게재됐다. 데이터 센터의 인증을 담당하던 RSA는 2011년에 해킹을 당했고 이때 일회용 인증 비밀번호(One Time Password)와 관련된 주요 기밀 정보가 유출되어 록히드마틴 해킹에 악용됐다. 2015년에 이미 에드워드 스노든이 미군 전투기 설계도를 포함한 정보 유출 사실을 일반에 공개한 바 있지만, 해당 사건 발생하고 10년이 지난 후에야 당시 국가안보국(National Secu-

2) The Full Story of the Stunning RSA Hack Can Finally Be Told (WIRED, 2021.05)

rity Agency, NSA) 국장이 중국 상하이 인근 인민해방군 부대의 침투 시도를 인정한 것이다(Andy 2021).

2021년 바이든 대통령이 취임한 이후 미국은 일련의 사이버공격을 받았으며, 특히 5월 미국 남동부 지역의 약 45%에 해당하는 8,850㎞에 석유 공급이 중단되는 큰 피해가 있었다. 랜섬웨어 공격으로 미국 최대 송유관 관리 업체인 콜로니얼 파이프라인(Colonial Pipeline)의 IT 비즈니스 시스템이 중단되어 휘발유 가격이 치솟고 지역 주유소의 약 65%가 문을 닫자, 바이든 대통령은 국가 비상사태를 선포하였으며(Keith and Harriet 2021), 랜섬웨어 공격의 이틀 후인 5월 12일 '국가 사이버보안 개선에 관한 행정명령(EO-14028)'을 발표했다.

이러한 공급망 사이버공격이 사회적 이슈가 되는 이유는 1) 공급자와 소비자의 정상적인 계약 관계를 악용하여 방어 체계를 무력화시킴으로써, 공급 체계의 신뢰성을 약화하는 효과와 이에 따라 그동안 2) 내부 시스템에 설치된 HW와 SW만 책임 범위라는 인식이 생태계 가치사슬(Value Chain)을 공유하는 공급망까지 확대되었기 때문으로 분석된다. 내부가 아닌 외부 조직의 행위로 인해 손해 볼 가능성을 뜻하는 '제3자 위험(3rd Party Risk)'은 SW 공급망에서 경계선(Perimeter) 방어 전략의 한계를 노출했다. 이렇게 타사 시스템 또는 취약한 구성요소의 종속성 위험을 이용한 공격은 피해 당사자의 직접적인 제어가 불가능한 영역에서 발생하여, 경계선 방어만으로 피해를 예방하기가 불가능하다(최윤성 2022).

2. 공급망의 취약성과 경제안보

카네기(Carnegie) 국제평화재단은 'ICT 공급망 무결성: 정부와 기업 정책을 위한 원칙'이라는 보고서에서 공급망 문제가 지정학, 스파이 활동, 경쟁 및 상업주의, 소비자 보호와 매우 복잡하게 연결되어 있어 일부 정부나 기업이 느슨한 보안 표준이나 제품 및 서비스의 보안 취약점과 같은 결함을 악용하여 공급망에 고의로 개입하는 것을 숨길 수 있다고 했다. 또한 늘어나는 외부 연결과 오픈소스 SW 사용 등으로 인해 공급망 공격 표면이 증가하면 국가 배후의 위협 행위자가 의도적인 백도어(Backdoor)[3]를 삽입할 수 있고, 이를 통해, 디지털 제품 및 서비스의 무결성에 대한 '신뢰'가 떨어질 수 있다고 분석했다(Ariel 2019).

관련 사례로 2018년 블룸버그(Bloomberg)는 중국이 마이크로칩(Microchip)을 사용해 미국의 주요 기업에 침투한 방법에 대한 'The Big Hack'이라는 제목의 보고서를 발표했다. (Jordan and Michael 2018) 해당 보고서에서 피해자로 지목된 애플은 즉각 해당 사실을 부인했고, 당시 보고서의 신빙성이 확인되지 않았음에도 가해자로 지목된 슈퍼마이크로(Supermicro)의 주가는 40% 이상 급락했다(Kate 2018).

우리도 2018년 북한이 개발한 안면인식 보안 프로그램을 국내에

3) 백도어는 일반적인 인증과 암호화를 우회(bypassing)해 원격 접속 및 암호화된 텍스트에 대한 권한을 취득하는 등 은밀히 악성코드를 실행하는 전형적인 방법이다. 백도어는 설치된 프로그램의 형태를 취하기도 하고, 기존 프로그램 또는 하드웨어의 변형일 수도 있다. 일반적으로 CCTV에 깔려서 정보를 빼어갈 수도 있다. [Wikipedia]

납품하고 군사기밀을 빼돌린 혐의로 대북 사업가가 재판에 넘겨진 사례가 있었다. 해당 북한의 안면인식 프로그램이 납품되는 과정에서 북한이 심어놓은 악성코드가 국내 민간업체 등에 그대로 전파된 것으로 조사됐다(김계연 2018).

최근 몇 년간 미국 정부는 중국 화웨이(Hwawei)와 ZTE의 제품 및 서비스에 대한 사용 금지에서 중국에 기반한 기술 기업으로 대상을 확장하고 있다. 이에 중국도 지난 5월 미국 최대의 메모리 반도체 기업인 마이크론(Micron) 테크놀로지가 국가안보를 위협한다며 제재안을 발표했다. 중국은 성명에서 "검토 결과, 마이크론의 제품이 심각한 네트워크 보안 위험을 초래하는 것으로 나타났다"며, "이는 중국의 중요 정보 인프라 공급망에 심각한 보안 위험을 초래하고 중국의 국가안보에 영향을 미친다"고 밝혔다. 그러나 정확히 어떤 위험이 있는지 또는 어떤 마이크론 제품에서 이러한 위험이 발견되었는지 등 자세한 내용은 제공하지 않았다(BBC 2023/05/22).

2024년 6월, 미국 상무부(Department of Commerce, DoC)는 데이터 도난 및 스파이 활동, 시스템 오작동, 악성 소프트웨어 설치로 인한 잠재적인 국가안보 위험을 이유로 미국 내 카스퍼스키(Kaspersky) 소프트웨어 제품 사용을 금지했다. 이는 러시아에 본사를 둔 사이버보안 회사의 미국 자회사인 '카스퍼스키랩(Kaspersky Lab, Inc)'이 대상이다. 또한 이 조치는 영국에 본사를 둔 'Kaspersky Labs Limited'도 같은 금지 대상 목록에 추가했다(Sara 2024).

한편 메신저 앱 '라인'을 둘러싼 소유권 분쟁 사태는 지난해 사이

버공격으로 악성코드에 감염된 후 네이버 클라우드와 일부 시스템을 공유했던 라인에서 51만 명의 개인정보가 유출되면서 촉발되었다. 네이버 클라우드는 일본 기업 트렌드마이크로(Trend Micro)가 개발한 보안 제품을 사용하고 있다. 트렌드마이크로의 보안 제품은 트렌드마이크로가 추천하는 국내 협력사와 계약을 맺어야만 사용할 수 있으며, 지난 6월 라인 야후 데이터 유출 사고의 원인이 된 악성코드 감염은 트렌드마이크로 협력사 직원 소유의 PC에서 발생했다. 일본 총무성은 복잡한 계약 관계로 책임이 불분명함에도 라인에 두 차례에 걸쳐 행정지도를 내렸고, 이는 네이버의 라인 영향력을 축소하려는 시도로 읽히며 한일 갈등의 신호탄이 되었다. 일본 정부의 논리는 보안 사고 이후, 한국 기업에 대한 과도한 의존도를 낮추기 위해 지배구조를 개편해야 한다는 것이었다. 라인 야후는 네이버와 일본 소프트뱅크가 50%씩 지분을 소유한 중간 지주회사 A홀딩스가 지배하고 있다(심우삼 2024).

이렇게 공급망의 취약성은 정치적, 경제적 이유로 과장되어 불안감을 높이며, 경쟁을 부추겨 시장을 분열시키고, 비용을 증가시켜 혁신을 억제하는 등 비생산적인 역학 관계로 이어질 수 있다(Ariel 2019). 미국의 교육기관인 상스 인스티튜트(SANS Institute)는 사이버 범죄의 투자 수익률(ROI)[4]에 관한 게시물에서 전 세계 사이버 범죄의 경제적 영향이 10년 동안 250% 증가하여 2025년에는 일본 전체 경제 규모의 2배가 넘는 105억 달러에 이를 것을 예측했다(Brie 2023). 이처럼 공

4) https://www.sans.org/blog/the-new-financial-metric-for-cybersecurity/

급망 사이버보안 문제는 경제 및 국가안보에 매우 중요하며, 지정학적 긴장은 공급망 환경을 더욱 복잡하게 만들고 있다. 강대국 경쟁이 부활하고 지정학적 위기가 고조되는 가운데 "경제안보가 곧 국가안보(Economic security is national security)"라는 경제의 안보화 추세는 강화되고 있다(차정미 외 2023).

특히 디지털 제품 및 서비스 공급망의 무결성이 여러 면에서 취약하고 빠르게 신뢰를 잃을 수 있기에 앞으로 신뢰할 수 있는 공급자의 역할은 더욱 중요해질 것이다. 국가적 차원에서 공급망에 대한 신뢰 부족은 경제에 부정적인 영향을 미치므로 공급과 수요를 안정화하기 위해 신뢰할 수 있는 공급자를 선제적으로 발굴하는 것이 필요하다. 이를 위해 주요국은 기존 산업 표준을 강화하고, 제3자를 통한 디지털 제품 및 서비스 결함의 악용을 사전에 방지하는 새로운 위험관리 체계를 마련하고 있다.

Ⅲ. 미국의 조달 체계 개선을 통한 공급망 위험관리

1. 국가 사이버보안 개선에 관한 행정명령 (EO-14028)

2021년 5월 발표된 미국 바이든 정부의 행정명령(Executive Order, EO) 14028을 기점으로 "연방정부에 납품되는 SW에 무엇이 들었는지 모른다는 기업은 신뢰하지 않겠다"는 SW 책임성을 강조하고 있으

며, 특히 SBOM 공유를 통해 SW 공급망의 투명성을 강화하는 측면이 드러나 있다.

SBOM은 기본적으로 SW 구성요소 간의 의존성(Dependency)을 나타내는 트리(Tree) 구조의 데이터 형식이다. 2021년 Log4j[5] 보안 취약점 사고 당시 어떤 시스템에 어떤 보안 취약점이 있는 SW 구성요소가 사용되는지 파악하기 어려웠던 문제를 해결할 수 있으며, SBOM 투명성을 기반으로 확보된 시스템 가시성은 SW 취약점 검증 업무의 자동화를 돕고, 향후 사이버보안 위험관리 및 의사결정을 위한 인텔리전스(Intelligence)를 제공할 것으로 기대된다.

또한 오픈소스 SW의 지식재산권 보호 및 컴플라이언스, 인공지능 시스템에서 사용되는 기계학습(Machine Learning) SW의 안전성 문제, 글로벌 클라우드 시스템에서의 서비스형 SW(SW as a Service) 책임성 등의 이슈를 해결하기 위한 기반으로써 SW 구성요소 수준의 투명성을 확보하여 SW 신뢰를 강화하려는 움직임도 증가하고 있다.

이러한 행정명령 'EO-14028 섹션 4'의 이행을 위해 상무부는 연방기관에 SW 제품을 납품하는 공급자에게 안전한 SW 개발, 증빙 및 SBOM 제출 방안 등을 담은 가이드를 배포하도록 했다(Joseph 2021). 이에 2022년 상무부 산하기관인 국립표준기술연구소(National Insti-

5) Log4j는 Java/Kotlin/Scala/Groovy/Clojure 언어로 만든 프로그램의 로그를 기록해 주는 라이브러리로, 이클립스, IntelliJ IDEA, 안드로이드 스튜디오 등에 추가해서 실행 시 자동으로 지정한 경로에 로그를 저장한다.

tute of Standards and Technology, NIST)는 '안전한 SW 개발 프레임워크(SSDF)'[6]와 '공급망 사이버보안 위험관리 가이드(C-SCRM)'[7]을 제작해 공개했다.

2. 안전한 SW 개발 관행을 통한 SW 공급망 보안 개선

2022년 9월, 연방기관이 상무부가 배포한 가이드를 준수하도록 하는 업무를 담당하는 백악관 관리예산처(Office of Management and Budget, OMB)는 '안전한 SW 개발 관행의 확립을 통한 SW 공급망 보안 강화에 관한 각서(M-22-18)[8]'를 발표했다. 각서의 핵심은 연방정부에 SW를 납품하려는 공급자에게 NIST의 SSDF 및 SW 공급망 보안 지침[9]에 명시된 안전한 SW 개발 관행을 준수한다는 자가 증명(Self-attestation)을 제출하도록 요구하는 것이다.

각서에 따라 연방기관은 SW를 사용하기 전에 개발사로부터 해당 SW가 NIST 가이드를 준수한다는 '자가 증명 양식'을 수령하고, 필요한 경우 SSDF 준수에 대한 추가 증거도 요구할 수 있다. 이 양식에는 최소한 SW 개발사의 이름, SW 제품에 대한 설명, SSDF 준수에 대한

6) Secure Software Development Framework v1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities

7) Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

8) M-22-18: Enhancing the Security of the Software Supply Chain through Secure Software Development Practices

9) SW Supply Chain Security Guidance Under EO 14028 Section 4e

진술이 포함되어야 한다. 연방기관은 필요한 경우 제3자 평가를 요구할 수 있으며, 추가 증거로 SBOM, 소스 코드 무결성 보증, 보안 취약점 수정 조치 목록을 포함할 수 있다. 이 정책의 배경에는 제3자 위험을 포함한 공급망 사이버보안을 보장하기에 기존 SW 공급자와의 계약이 불충분하다는 인식에서 비롯됐다.

이후 OMB는 두 달간의 의견수렴 과정을 거쳐 자가 증명 양식의 초안을 공개했으며, 2023년 6월에는 연방기관과 민간 부문으로부터 받은 의견을 바탕으로 기존 각서를 업데이트한 두 번째 각서(M-23-16)[10]를 발표했다. 이를 통해 증명 양식 제출 기한은 공통 양식의 최종 승인 이후로 연장되어 중요(Critical) 기능을 수행하는 SW의 경우 양식 최종안의 승인 3개월 이후, 모든 납품 SW의 경우 6개월 이후로 수정되었다. 또한 SW에 포함된 타사 오픈소스 및 상용 SW 구성요소는 자가 증명 양식의 제출 및 책임 범위에서 제외되었다.

3. 자가 증명(Self-attestation) 제도와 연방 법률

증명(Attestation)이란 "공식적으로 사실이라고 하는 공식적인 진술"[11] 또는 "사실 또는 진위에 대한 공식적인 검증"[12]을 의미하는 법률 용어로, 공통 양식에 서명하여 그 내용과 관계된 사람들이 적절하

10) M-23-16: Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices

11) 'formal statement that you make and officially say is true' [Cambridge]

12) 'an official verification of something as true or authentic' [Merriam-Webster]

게 따랐음을 확인하기 위한 절차를 말한다. 바꿔 말하면 SW 제조사가 자가 증명 양식을 작성하는 것은 자신이 제공하는 정보가 거짓이 아님을 스스로 확인하는 것이다.

미국 연방법인 '허위 진술(Making False Statement, Title 18 USC § 1001)'은 연방정부에 제출하는 문서에서 중요한 사실을 고의로 위조하거나 은폐하는 행위를 범죄로 규정하며, 위반할 경우 최대 25만 달러의 벌금 또는 5년 이하의 징역형에 처할 수 있다. 또한 '부정 청구법(False Claims Act, Title 31 USC § 3729)'은 연방정부로부터의 승인 또는 대가를 얻을 목적의 고의로 허위 정보를 제출한 경우, 민사적 배상으로 최대 1만 달러와 정부가 입은 손해의 3배에 해당하는 벌금을 부과할 수 있도록 규정하고 있다. 내부 고발자 보상 제도의 일종인 이 법은 모든 미국 시민이 허위 또는 사기로 정부에 손해를 끼친 개인이나 회사를 고소할 수 있도록 허용하며, 정부는 소송을 지원하고 중재 또는 법원 판결로 인한 환수액의 최대 30%를 고발자에게 지급할 수 있다.

일례로 세계 최대 제약회사인 화이자의 자회사인 와이어스(Wyeth)는 영세민을 위한 공공 의료 프로그램인 메디케이드(Medicaid)에 의약품 비용을 부풀려 청구한 혐의로 미국 법무부로부터 부정 청구법에 따른 소송을 당했고, 징벌적 손해배상으로 의약품 비용의 3배 이상을 배상하라는 판결을 받았다(최병국 2016).

이와 관련해 SW 제조사가 자가 증명 양식에 허위 정보를 제공할 경우 연방 법률에 따라 처벌을 받을 수 있고 민사상 손해배상 책임도

질 수 있어, 연방정부에 제출하는 '자가 증명'은 단순한 확인이나 신고의 의미를 넘어 법적 구속력이 있는 문서로 간주할 수 있다. 2023년 7월에 발표된 미국 국가 사이버보안 전략(National Cybersecurity, Strategy, NCS)의 실행 계획에도 EO-14028에 기반한 연방 조달 규정(Federal Acquisition Regulation, FAR)의 이행과 공급자 사이버보안 강화를 위한 부정 청구법의 적용 계획이 포함되어 있다(White House 2023).

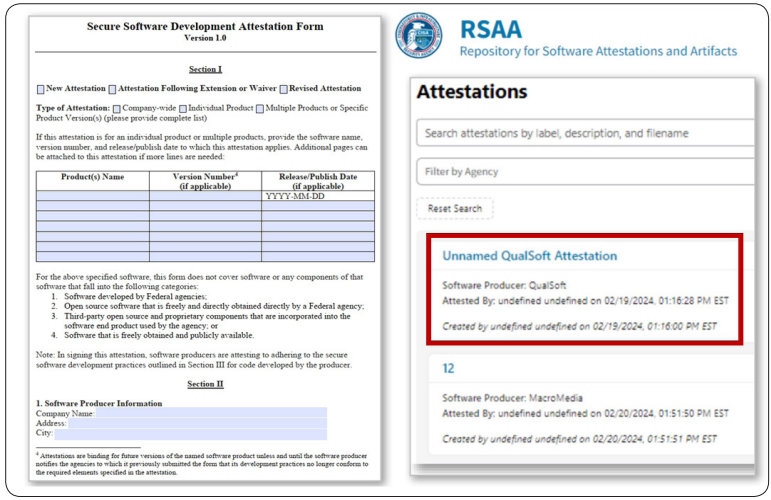
4. 안전한 SW 개발의 책임성 강화

2024년 3월, OMB와 사이버보안 및 인프라 보안국(Cybersecurity & Infrastructure Security Agency, CISA)은 '안전한 SW 개발 증명 양식(Secure Software Development Attestation Form, SSDAF)'이라는 자가 증명 양식 최종안을 발표했다. CISA는 SSDAF를 '최소한의 안전한 개발 기법과 도구의 활용을 지원하는 양식'으로 규정하고, 6월부터 중요(Critical) SW, 9월부터는 납품되는 모든 SW로 대상을 확대한다. SW 제조사, 제품명, 버전, 증명 일자 등의 정보를 〈그림 2〉의 PDF 양식에 담아 각 연방기관 담당자 이메일 또는 온라인으로 제출할 수 있으며, 이를 위한 웹사이트(RSAA)[13]와 가이드[14]가 제공된다(CISA 2024).

13) Repository for Software Attestations and Artifacts (https://softwaresecurity.cisa.gov)

14) https://www.cisa.gov/sites/default/files/2024-03/CISA_RSAA_User_Guide_18_March_2024.pdf

〈그림 2〉 SSDAF 증명 양식과 RSAA 웹사이트 예시



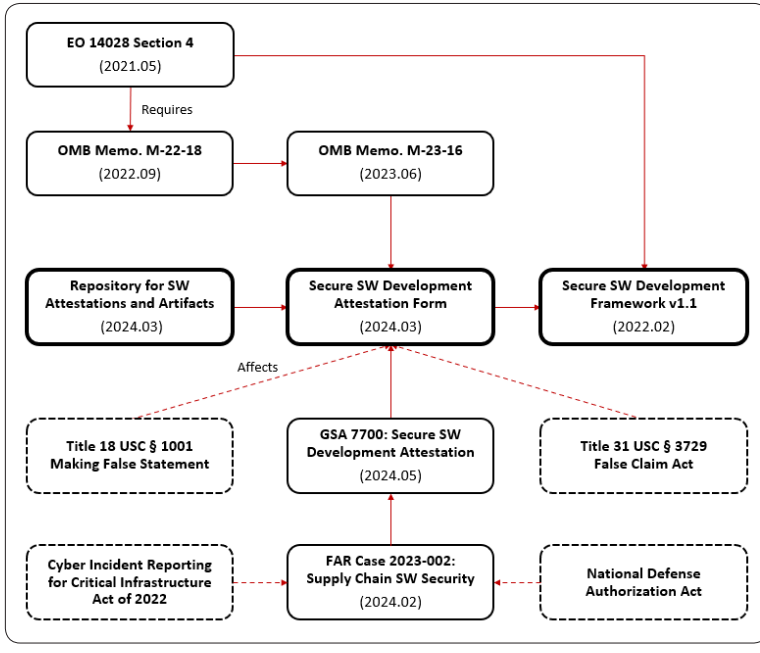
출처: 사이버보안 및 인프라 보안국(CISA)

참고로 2024년 7월, 미국 증권거래위원회(SEC)는 솔라윈즈 社의 정보보호 최고책임자(Chief Information Security Officer, CISO)를 기소했지만, 투자자를 오도했다는 사기 혐의의 대부분은 법원에서 기각되었다(Sam 2024). SEC가 사기 및 내부통제 실패로 기업의 CISO를 기소한 것은 이번이 첫 번째 사례이지만, 향후 '자가 증명' 제도를 통해 정부에 SW를 공급하는 기업은 사이버보안과 안전한 SW 개발 환경을 입증하기 위한 SW 증거(Artifact) 관리에 더욱 주의를 기울여야 한다.

SSDAF의 핵심은 SW 공급망 보안 강화를 위한 NIST 가이드(SSDF 및 SW Supply Chain Guide)의 준수 여부를 자체 인증하는 것이다. 추가 정보(Additional Information)로 분류되었던 SBOM은 SSDAF 최종안의

직접적인 요구 항목에서 제외되었지만, 연방기관에 따라 특정 지침으로 추가될 수 있다. 이때 SBOM은 단순한 데이터 형식을 넘어 실사(Due diligence)의 척도 및 SW 품질 보증을 입증하는 수단으로서 구매자와 신뢰할 수 있는 공급자를 연결하는 기술이 된다.

〈그림 3〉 미국 EO-14028 이후 SW 공급망 보안 체계 강화 흐름도



출처: 저자 작성

5. 행정명령과 조달 체계 개선 흐름

우리 조달청과 유사한 미국 연방조달청(General Services Administration, GSA)은 연방정부 기관에 상품 및 서비스를 공급할 책임이 있다.

연방정부 조달에 관한 책임과 권한은 개별 부처와 정부 기관에 있지만 모든 정부 부처는 FAR을 준수해야 한다. 2023년 10월부터 12월까지 GSA는 국방부(Department of Defense, DoD) 및 미 항공우주국(National Aeronautics and Space Administration, NASA)과 공동으로 FAR 개정을 위한 공개 의견 수렴 절차를 진행하였다.

〈표 1〉 EO-14028 이후 SW 조달 개선 프로세스 타임라인

시기 (관련 부처)	제목 (식별 번호)	주제	공급망 비고
2022-09 (OMB)	집행 부서 및 기관장을 위한 각서 (M-22-18)	안전한 소프트웨어 개발 관행을 통한 소프트웨어 공급망의 보안 강화	SW 제조사로부터 자가 증명을 받고, SBOM을 수집하며, NIST 공급망 보안 지침을 준수
2023-06 (OMB)	집행 부서 및 기관장을 위한 각서 (M-23-16)	[M-22-18]에 설정된 요구사항을 강화하고 중요성을 재확인 및 업데이트	제3자 구성요소는 SW 최종 제작자로부터 증명을 수집, 보안 관행의 증명이 어려운 경우 POA&M[15] 제출
2023-10 (GSA, DoD, NASA)	사이버 위협 및 사고 보고 및 정보 공유 (FAR Case 2021-017)	연방 계약업체를 위한 사이버 위협 및 사고 보고와 정보 공유에 관한 EO를 부분 시행하고 관련 사이버보안 정책을 시행하기 위해 FAR을 개정할 것을 제안	연방 계약업체에 대한 사이버 위협 및 사고 보고를 강화하기 위해 FAR 개정안을 제안, 사이버보안을 개선하기 위해 정부와 민간 부문 간의 정보 공유의 중요성을 강조
2023-10 (GSA, DoD, NASA)	분류되지 않은 연방 정보 시스템에 대한 사이버보안 요구사항 표준화 (FAR Case 2021-019)	미분류 연방 정보 시스템에 대한 연방기관 전반의 사이버보안 계약 요건을 표준화하기 위한 EO와 국가의 사이버보안 개선에 관한 법령을 부분 시행하기 위해 FAR 개정 제안	보안 사고와 관계없이 계약에 사용되는 모든 SW에 대해 SBOM을 개발 및 유지한다는 요건을 제안, 2023년 12월 4일까지 제안된 규칙에 대한 의견을 제출

시기 (관련 부처)	제목 (식별 번호)	주제	공급망 비고
2024-01 (GSA)	GSA 인수 인력을 위한 각서 (MV-23-02)	GSA에서 승인된 소프트웨어만 획득하고 사용하도록 보장	IT 표준 프로세스를 통해 승인된 SW는 GEAR[16] 플랫폼에 게시되며, 향후 FAR 규칙이 확정되면 GSA 정책도 업데이트될 예정
2024-02 (GSA, DoD, NASA)	공급망 소프트웨어 보안 (FAR Case 2023-002)	연방기관에서 구매할 수 있는 SW 공급업체가 국토안보부 CISA의 보안 소프트웨어 개발 증명 양식과 중요 SW에 대한 요구사항을 준수하도록 요구	행정명령 14028 "국가의 사이버보안 개선"의 섹션 4(n) 및 4(k)와 관리 예산처 각서 22-18 및 23-16에 따라 발행
2024-03 (DHS, CISA)	안전한 SW 개발 증명 양식 최종안 (OMB Control #: 1670-0052)	2022년 9월 14일 이후 개발된 소프트웨어 또는 주요 버전 변경이 있는 SW에 대해 자가 증명을 요구 (24년 6월부터 중요 SW, 9월부터 모든 SW 제출)	증명에는 SW 개발 환경의 보안, 신뢰할 수 있는 소스코드 공급망 유지, 자동화된 도구를 통한 보안 취약점 검사 등이 포함

출처: 저자 작성

이를 통해 사이버 사고 대응에 있어 알려진 취약점의 원인을 신속하게 식별할 수 있는 SBOM의 중요성이 강조되었으며, 공급망 보안과 관련하여 논의된 주요 사항은 다음과 같다.

1) 첫 번째로 계약업체가 계약 수행에 사용되는 각 컴퓨터 SW에 대한 SBOM을 개발하고 유지해야 함

15) Plan of Action and Milestones (실행 계획 및 마일스톤)

16) GSA's Enterprise Architecture Analytics & Reporting (GEAR)

2) 새로운 정보 공유 구조(Mechanism)를 포함하여 해외에서 활동하는 계약자 및 하청업체에 대한 규정 준수 조치를 다룸

또한 '중요 기반 시설에 대한 사이버 사고 보고법(CIRCIA)'[17]의 적시 적용에 대해 언급하고 관련 기관 및 업계의 의견을 수렴했다.

1) 계약업체는 보안 사고가 발생했을 수 있는 모든 지표를 신속하고 철저하게 조사하고, 발견 후 8시간 이내에 이를 완료하도록 요구함
2) 이후 계약자, 기관 및/또는 조사 기관이 모든 근절 또는 개선 활동을 완료할 때까지 72시간마다 제출물을 업데이트해야 함

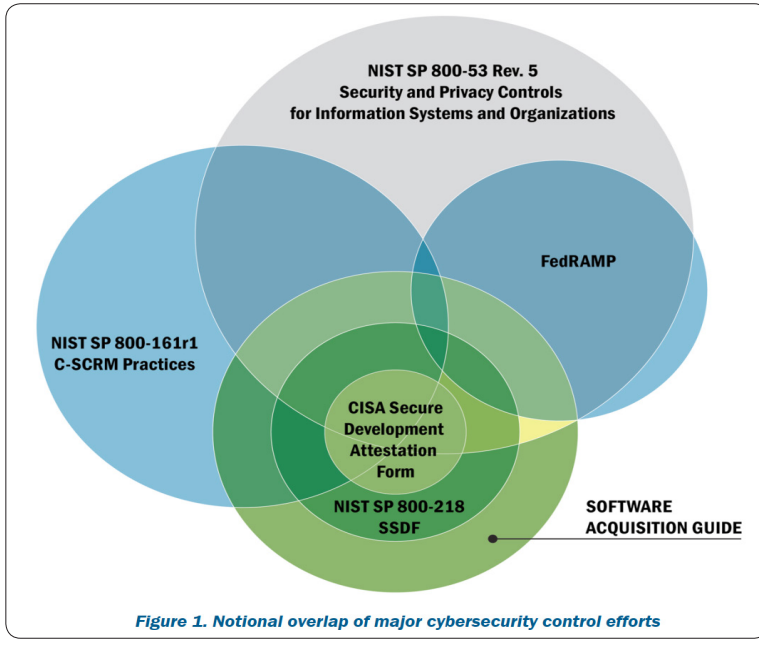
2024년 4월, GSA는 FAR에 향후 공급망 정책 및 절차를 수립하기 위한 규칙을 발표했다. 이 규칙은 올해 말 GSA, DoD, NASA가 제품 및 서비스를 획득할 때 정보보안 및 공급망 보안을 관리하기 위한 정책과 절차를 포함하는 새로운 'FAR 파트 40'을 제정하는 개정안으로 처리될 예정이다.

참고로 제안된 수정안은 2019 회계연도 국방수권법(NDAA)[18] 섹션 889의 요건과 유사하다. 섹션 889는 연방정부의 화웨이 및 ZTE 장비와 서비스 사용을 두 부분으로 나누어 금지하고 있으며, 파트 A는 정부 내부 사용에 적용되고 파트 B는 이러한 요건을 연방 계약업체

17) Cyber Incident Reporting for Critical Infrastructure Act of 2022

18) National Defense Authorization Act

〈그림 4〉 미국 사이버보안 통제 간의 관계 도식화



출처: SW Acquisition Guide for Government Enterprise Consumers (CISA, 2024)

로 확대한다. 또한 국토안보부(DHS)와 CISA의 SSDAF 및 중요 SW에 대한 요건을 준수해야 한다. 이 규정은 현재 규칙 제안 단계에 있으며, 2024년 9월까지 규칙 제정 제안 공지가 공개되어 있다(GSA/DoD/NASA 2024).

2024년 8월, CISA는 민관합동 ICT 공급망 위험관리 태스크포스(Task Force)가 개발한 'SW 구매 가이드'[19]를 발표했다. 이 가이드는

19) Software Acquisition Guide for Government Enterprise Consumers (ICT SCRM TF)

정부·공공기관과 기업의 구매 책임자, 조달 조직, CIO, CISO 등이 SW 생명주기에 대한 공급업체 보안 관행을 이해, 평가 및 측정하는 데 활용하기 위한 것으로, SW 공급망과 관련된 조달, 배포 및 운영에 적용할 수 있다. 해당 가이드는 총 77개 통제 항목이 5개 섹션으로 나뉘어 구성되어 있으며, 〈그림 4〉에 표현된 것처럼 '안전한 SW 개발 증명 양식(SSDAF 또는 GSA 7700)'에 서명함으로써 25개 통제 항목 적용이 면제되는 등 타 가이드 및 인증 프로그램과의 연계성을 제공한다(SwA WG 2024).

Ⅳ. 국내 공급망 사이버보안 현황 검토

1. 국가 사이버안보 전략 및 기본계획

2024년 2월 국가안보실과 관계부처 합동으로 마련된 '국가 사이버안보 전략'은 사이버안보 분야 최상위 지침서로, 5대 전략과제를 제시하고 있다. 또한 국가안보실은 국정원, 외교부, 국방부, 과기정통부, 검·경 등 14개 정부 부처와 협력해 더 구체적인 실행 계획을 담은 '국가 사이버안보 기본계획'도 발표했다. 이중 전략과제 3번, '국가 핵심 인프라 사이버 복원력 강화'와 전략과제 5번, '업무 수행기반 강화'에서 제시된 공급망 보안 세부 실행 계획은 〈표 2〉와 같다.

〈표 2〉 국가 사이버안보 전략 및 기본계획의 공급망 과제

전략과제	구분	세부 계획
3. 국가 핵심인프라 사이버 복원력 강화	다. 범국가적 차원의 ICT 공급망 보안정책 및 대응체계 확립	**국가 사이버안보 전략:** 1) 정부 ICT 제품 및 부품의 조달 과정에 대한 보안성을 확보할 수 있도록 기존 보안 관련 제도 · 지침을 개정하고 신뢰할 수 있는 공급업체를 지정 · 관리할 수 있는 방안을 마련한다. 2) 소프트웨어 개발 시 보안 취약점을 최소화할 수 있도록 소프트웨어에 대한 구성 정보를 표준화하고 관리체계를 수립한다. 3) ICT 공급망 보안을 위한 교육 · 훈련, 지속적 관리 및 기술지원을 할 수 있는 역량과 환경을 구축한다.
		국가 사이버안보 기본계획: • SW 개발·공급 단계의 취약점 내재 위험성에 대응하고, 국내 SW 기업의 해외 무역장벽 극복을 위해 미국·유럽 등 주요국과 유사한 SW 구성요소 명세서(SBOM, SW Bill of Material) 도입을 지원 • 국가·공공기관에 도입되는 SW의 공급망 보안 관리체계를 강화하기 위해 범정부 합동으로 SW 공급망 보안 관련 제도·지침 정비 • 국가·공공기관에 도입되는 SW 구성정보 항목을 표준화하고 행정지원 디지털서비스의 설계·구현 단계 개발보안 적용 지원 강화 • SW 공급망 보안관리 중요성에 대한 인식 제고를 위해 국가·공공기관 대상 공급망 보안 관리체계 교육 및 기술지원 확대
5. 업무수행기반 강화	가. 국가 사이버 위협 대응 체계 정립	**국가 사이버안보 전략:** 3) 사이버공격 발생 시 신속하게 정부·기업의 핵심역량을 결집하기 위해 통합 대응 조직을 설치, 국가 차원의 합동대응 역량을 강화한다. 5) 관계부처·기관 및 기업 간 협업 강화를 위하여 범국가 차원의 '사이버안보 협력 플랫폼'과 허브를 구축한다.
		국가 사이버안보 기본계획: • 사이버안보 위협으로부터 국민안전 보호를 위하여 설치된 민관 합동 통합대응 조직(국가사이버위기관리단)의 역량 강화를 위해 외교·통일·교육 등 참여기관 확대 및 민간 전문업체와 협업·정보 공유 강화 추진 • 국가 사이버안보 위협정보 공유플랫폼(NCTI·KCTI) 고도화 및 사이버안보 관련 정보 교류·협력의 장으로 도약

전략과제	구분	세부 계획
5. 업무 수행기반 강화	다. 범국가적 사이버 위기 대응을 위한 민간 역량 활용 확대	**국가 사이버안보 전략:** 1) 민간 이해당사자 간 협력을 활성화하고 민간 주체의 자율적 · 능동적 참여를 촉진하는 협력적 플랫폼을 구축한다. 2) 사이버사고에 대응하는 정부와 기업 간 정보공유체계를 정비하여 취약점 정보, 사이버 위협징후 등 사이버안보 관련 정보를 신속하게 상호 공유하고 대처할 수 있도록 한다.
		국가 사이버안보 기본계획: • 사이버안보에 관한 민간 전문가의 전문지식 활용 및 의견수렴을 위해 국가사이버안보센터에 사이버안보자문단 설치·운영 • 사이버안보 정보 공유 범위 확대 등 민간기업·단체와 사이버안보정보 협력을 강화하여 범국가적 사이버안보 역량 강화 • 국내외 정보보호 기업과 긴밀한 정보공유·합동분석을 위해 협의체 및 플랫폼을 구축하고 합동근무 형태의 사이버위협분석센터 개소 • 다양한 산업 분야의 기업·기관이 정보통신망 침해사고에 적시 대응할 수 있도록 위협정보 분석·공유 체계 'C-TAS' 회원사 확대 등 활성화 추진
	라. 전문인력 양성 및 유지	**국가 사이버안보 전략:** 5) 공급망 보안 · 하이브리드 위협 등 복합적인 위험 요소들에 대한 예측 · 평가 · 대응을 위해 전문인력을 양성하고 교육 · 연구개발 등에 투자하여 근본적인 복원력을 강화한다.
		국가 사이버안보 기본계획: • 고도화되는 신기술 사이버위협에 대응할 수 있도록 맞춤형 교육·훈련을 통한 분야별 전문인력 양성·유지 체계 구축 • 민간 화이트해커의 신규 취약점 발굴과 신고를 장려하고 참여를 유도하기 위해 취약점 신고에 대한 보상을 강화 • 군 사이버전문인력 양성 및 전문성 제고를 위해 유관부처간 협력을 확대하고, 사이버전문사관 양성·교육 등 프로그램 강화 • 교육분야 정보보호 업무 담당자 전문성 강화를 위한 정보보호 교육센터 교육 콘텐츠 품질 개선, 실습 강화 등 운영 내실화 • 민간기업이 참여하는 사이버 위기대응 모의훈련을 내실화하고 민·관 협조체계를 지속 점검하여 사이버 위기상황 발생시 신속하게 대응 • 범국가 사이버방어 합동훈련을 통해 국가 전 영역을 위협하는 국제 및 국가배후 해킹 조직의 사이버공격을 방어할 수 있는 역량 확보 • 글로벌 사이버안보 위협에 대한 합동대응 역량을 제고하기 위하여 세계적 수준의 최첨단 국제 사이버훈련센터를 구축·운영

전략과제	구분	세부 계획
5. 업무 수행기반 강화	마. 대국민 인식 제고 및 실천 강화	**국가 사이버안보 전략:** 1) 국민들이 사이버안보의 중요성과 안전수칙을 체득할 수 있도록 SNS · 대중매체 등을 활용한 국민 참여형 인식제고 캠페인을 활성화한다. 2) 국민들이 사이버안보 위협에 대한 중요성을 인식하고, 일상에서 사이버위협에 노출되지 않도록 맞춤형 인식제고 프로그램 및 콘텐츠를 개발 · 제공한다.
		국가 사이버안보 기본계획: • SNS·영상물 등을 활용한 국민 참여형 정보보호 인식 제고 캠페인 추진, 일상 속 정보보호 실천을 장려하고 국민 경각심 고취 • 금융이용자 침해사고 피해 예방을 위한 대국민 보안인식 제고 활동 추진 • 정보보호의 날·달 행사를 통해 정보보호 및 사이버안보에 기여한 유공자를 발굴·포상하고, 범국민 정보보호 인식제고 기회로 활용 • 사이버안보 국제행사 '사이버 서밋 코리아(CSK)' 정례화를 통해 글로벌 사이버안보 선도 국가로서 책임을 다하는 대한민국의 노력을 대외 공표

출처: 2024 국가 사이버안보 전략 및 기본계획 (저자 요약)

2. 경제안보를 위한 공급망 안정화 지원 기본법

경제안보라는 말이 단순히 '공급망 안전'이라는 좁은 개념을 넘어 산업정책, 재정지원, 국방산업 등에 대한 정부의 관심과 보조금으로 연결되는 '마법의 단어(magic words)'가 되고 있다. 개별 국가들은 변화된 환경 속에서도 원래 하고자 하는 국가의 중장기 목표와 과제에 새롭게 활력을 불어넣는 프레임으로 경제안보를 활용 중이며, 국가마다 중장기 목표와 직면한 위협의 내용이 다를 수 있다는 점에서 경제안보 전략과 거버넌스에 차이가 발생한다. 또한 우리가 처한 위기

와 기회를 객관적으로 평가하고, 중장기 국가전략과 연계하여 경제안보 개념, 경제안보 전략의 목표와 비전을 명확히 하며 이를 토대로 한국 특색의 복합적 경제안보 전략과 거버넌스를 고민하고 설계해 나갈 필요가 있다(차정미 외 2023). 경제안보의 관점에서 우리나라는 핵심 자원·광물, 첨단 전략기술, 산업 공급망 및 사이버안보, 보건·의료 영역에서 구조적으로 취약하며, 오픈소스 기반 정보통신 인프라 비중이 높은 우리 현실에서 주요 정보통신 기반 시설 및 공급망에 대한 사이버 위협 수준도 높은 편이다(김상배, 유지연 외 2022).

지난 6월 27일, 사이버보안을 경제안보 서비스로 지정하고, 탄력적인 공급망 확보를 위한 사이버 위협 예방 및 대응을 강조하는 '경제안보를 위한 공급망 안정화 지원에 관한 기본법(이하 기본법)'이 시행됐다. 이는 디지털 인프라의 안정적인 운영을 위해 IT 부품, 기기, SW를 필수 원재료로 인식하고 공급망 위기[20] 예방을 위한 사이버보안 서비스의 안정적 제공을 지원한다.

기본법은 경제안보를 국가와 국민의 안전보장 유지와 경제활동에 지장이 초래되지 않는 상태로 정의[21]하며, 관계부처 합동으로 구성된

20) '공급망 위기상황'이란 공급망이 정상적으로 작동하지 아니함으로써 국가 및 국민의 경제활동에 심각한 피해가 발생하거나 발생할 우려가 있어 국가가 긴급하게 대처할 필요가 있는 상황을 말한다. [기본법 제2조]

21) '경제안보'란 국내외에서 발생하였거나 발생할 가능성이 있는 경제·통상·정치·외교적 상황 변화나 자연재해 등에도 불구하고 국내의 생산, 소비, 유통 등 국가 및 국민의 전반적인 경제활동에 필수적인 품목, 서비스, 기술 등이 원활히 유입되고, 부적절하게 해외로 유출되지 아니하도록 함으로써 국가의 안전보장이 유지되고 국가 및 국민의 경제활동에 지장이 초래되지 아니하는 상태를 말한다. [기본법 제2조]

'공급망 안정화 위원회'가 공급망 안정화[22] 정책 및 지원에 관한 기본계획을 2024년 하반기까지 확정하면 소관 부처는 연도별 시행계획을 2025년 1월까지 수립한다. 이를 통해 공급망 안정화를 위한 선제적 위험 평가와 위기 대응 조치가 포함된 3년 단위의 기본계획이 마련될 예정이다(기획재정부 2024).

3. 미국의 공급망 사이버보안 개선 흐름과의 비교

미국 백악관은 사이버보안을 강화하고 사이버 공간의 복원력을 보장하기 위한 국가 사이버보안 전략(NCS)을 2023년 3월에 발표하고 같은 해 7월에는 세부 실행을 담은 이행 계획(Implementation Plan)을 발표하였다. 본 고에서 설명하는 미국의 조달 개선 노력은 OMB 각서 및 이행 계획 발표 이후에 진행되었으며, 우리는 올해 국가 사이버안보 전략 및 기본계획이 시행됨에 따라 공급망 보안 정책의 시작 단계에 있다.

정부는 올해 5월 발표한 'SW 공급망 보안 가이드라인 1.0'을 통해 산업 생태계별 SW 공급망 보안 지원 거점을 마련하고 민간 중심의 SBOM 활성화 및 위험관리 체계를 통해 SW 공급망 위기 발생 시 신속한 대응이 가능하게 할 계획을 발표했으며, 과학기술정보통신부도 SW 공급망 보안 관리 적용·확산을 위해 내년도 예산을 신규 편성했

22) '공급망 안정화'란 공급망의 안정적 유지를 저해하는 위협요인의 예방 · 대비 · 대응을 포함하여 공급망의 탄력적 회복 능력을 확보하기 위하여 수행하는 모든 활동을 말한다. [기본법 제2조]

다(김영명 2024). 다만 국내 SBOM은 국가정보원의 'NIS-SBOM v1.0 (2024.05)', '공개 SW 공급망 관리를 위한 SBOM 속성규격(TTAK.KO-11.0309, 2022.12)' 등이 제정되었으나 아직 제도화 전 단계라 현장에서 활용되고 있지는 않다.

V. 맺음말

미국은 연방정부의 SW 조달 체계 개선을 통한 공급망 위험관리 체계 구현을 모색하고, 시스템 침해사고를 법·제도와 연계하는 '자가 증명' 제도와 사이버 복원력 확보를 위해 SW 투명성과 사이버보안 기술을 연결하는 'SBOM 기반 위험관리 체계'를 국제적 공급망 보안 정책으로 제시했다(ESF 2023).

이에 '자가 증명' 제도는 앞서 소개한 SEC의 솔라윈즈 기소 사례처럼, 기업이 법률 또는 사이버보안 위험을 회피할 목적으로만 변호사를 고용하는 것을 방지하고, 단기적인 이익을 위해 사이버보안 관리 책임에 소홀한 기업을 처벌함으로써 안전하지 않은 SW의 근본 원인을 제거할 수 있다고 미국 정부가 판단했음을 시사하는 것이다.

다만 SBOM 아이디어는 규제 기술로 활용될 만큼 충분히 성숙하지 않았고, 기존 SW 기업이 새로운 지침을 따르기 위해 보안 제품을 구매하는 등 추가 비용이 발생하기 때문에 지속적인 기술 개발과 산업의 수용이 필요하다(Michele 2023). 또한 SBOM은 특정 시점의 정적 스냅숏(Snapshot) 정보를 활용한 사후 대응형 기술인 만큼 실행 시간

(Runtime) 등 운영환경의 위험을 예방하기 위한 선제 대응형 기술과 상호 보완하는 연구가 필요하며, 초기 투자가 가능하고 보안 중요도가 높은 주요 핵심 산업, 공공기관, 국가·민간 부문의 주요 정보통신 기반 시설 등에 우선 적용하는 것이 적절하다.

공급망 위험은 글로벌 이슈이고, 공급망 공격에는 국경과 분야를 가리지 않는다. 우리는 공급망 보안 여정의 시작 단계에 있으며 앞으로도 많은 과제가 남아 있다. 안전한 공급망은 소비자, 공급자, 정부 모두에게 중요하므로 더 많은 참여자 간의 협력이 최우선 과제이다. 다음으로 국내 사이버보안 시스템만으로는 방어하기 어려운 제3자 위협에 대응하기 위해 공급망 위험관리를 기존의 방어 체계에 추가하고 점진적으로 확대해야 한다. 공급망 참여자들이 기존의 행동 패턴에서 벗어나기 위해서는 예산, 인력 등 자원에 대한 신규 투자와 함께 최고경영자의 변화 의지, 담당자 권한이 필수적이다(박춘식 2023). 또한 SW 생태계의 출발점인 SW 개발자를 위한 자동화 도구와 기술 지원도 필요하며, 취약점 관리 교육과 보안 인식 제고가 뒤따라야 한다.

이를 선도하는 SW 공급망 보안 제도는 관리 책임만 강조되고 개발자의 창의성은 억압되지 않도록 안전한 항구[23] 원칙에 따라 설계되어야 하며, 정부는 SW 단가 상승에 대비하여 상대적으로 자원과 기

23) 안전한 항구(Safe Harbor)란 규제 당국이 제시한 요건이나 기준을 충족하면 해당 규범을 준수한 것으로 보아 더 이상 위법한 것으로 취급하지 않는다는 원칙

술이 부족한 우리 SW 공급 기업에 유리한 방향과 지속적인 시장 유인책을 제공해야 한다. 종합하면 국가·공공기관의 제품 및 서비스 시장 도입의 관문인 국정원 '보안적합성 검증' 제도 등에 SW 공급망 위험관리 제도를 우선 적용하는 것이 타당하다.

국내 공급망 관리 측면에서 우리는 미국, EU, 일본 등 주요국보다 지리적으로 공급망이 작고 통제 범위와 대상이 적어 전반적인 공급망 신뢰도 향상에 유리하다. 또한 대부분의 기반 시설을 정부가 관리하고 있어 국가, 부문, 단위로 구성되는 국가 3선 보안관제 체계와 같이 중앙 집중적이며 신속한 위기 대응 시스템을 구성하는데 수월하다. 이는 우리나라가 향후 공급망 보안 문제를 해결하는 데 있어 다른 국가를 선도할 수 있는 또 다른 장점이라고 생각한다.

마지막으로 본 고는 디지털 공급망 보안과 관련된 다양한 연구, 보고서, 사건·사고를 참고 자료로 담았으며, 공급망 보안 전문가와 법·제도 연구자들이 서로 협력할 수 있는 매개체가 되길 희망한다.

〈참고문헌〉

최윤성. 2022. “미국의 소프트웨어 공급망 보안 정책 동향: SBOM 사례를 중심으로.” 『정보보호학회지』 제32권 제5호, 7-14.

Gopal Ratnam. 2021. “SolarWinds Hack Recovery May Cost Upward of $100B”, Government Technology (January 12).

Andy Greenberg. 2021. “The Full Story of the Stunning RSA Hack Can Finally Be Told.”, WIRED (May 20).

Joseph R. Biden JR. 2021. “Executive Order on Improving the Nation’s Cybersecurity (EO 14028).”, The White House. May.

Keith Griffith and Harriet Alexander. 2021. “Colonial Pipeline pumps gas again after Russian cyberattack shut it down for six days.”, Mail Online (May 13).

Ariel E. Levite. 2019. “ICT Supply Chain Integrity: Principles for Governmental and Corporate Policies.”, Carnegie Endowment for International Peace. October.

Jordan Robertson and Michael Riley. 2018. “The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies”, Bloomberg (October 10).

Kate Fazzini. 2018. “Chinese spy chips are found in hardware used by Apple, Amazon, Bloomberg says; Apple, AWS say no way”, CNBC. October 5.

김계연. 2018. “악성코드 숨긴 北프로그램 국내 납품…北서 원격설치도.” 『연합뉴스』 (9월 5일).

Sara Friedman. 2024. “Commerce Dept. finalizes determination to ban Kaspersky software due to national security concerns.”, Inside Cybersecurity (June 25).

BBC. 2023. “중국, 미 반도체 기업 ‘마이크론’ 제재 … ‘심각한 보안 문제’ 언급.” 『BBC 코리아』 (5월 22일).

심우삼. 2024. “라인사태 불러온 네이버 보안, 일본 업체가 담당했다.”, 『한겨레』 (6월 25일).

차정미, 배영자, 이정환, 오태현. 2023. “세계 경제안보의 실제와 한국 경제안보에의 제언: 경제안보 전략과 경제안보 거버넌스”, 국회미래연구원『국회미래의제』23-14호, 3.

Brie Entel. 2023. “The New Financial Metric for Cybersecurity.”, SANS Institute (Match 17).

최병국. 2016. “공룡기업들의 ‘나랏돈 도둑질’ 잡는 미국 부정청구법”『연합뉴스』(4월 30일).

The White House. 2024. “National Cybersecurity Strategy Implementation Plan Version 2.”, The White House, May.

Sam Sabin. 2024. “Most SEC charges dismissed in SolarWinds hack case.”, AXIOS (January 18).

CISA. 2024. “Secure Software Development Attestation Form Instructions.”, DHS-CISA, March.

Shalanda D. Young. 2022. “Enhancing the Security of the Software Supply Chain through Secure Software Development Practices.” EXECUTIVE OFFICE OF THE PRESIDENT, September.

Shalanda D. Young. 2023. “Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices.” EXECUTIVE OFFICE OF THE PRESIDENT, June.

GSA, DOD, NASA. 2024. “Federal Acquisition Regulation: Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems.” Federal Register Vol. 88, No. 190, October.

GSA, DOD, NASA. 2024. “Federal Acquisition Regulation: Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems.“ Federal Register Vol. 88, No. 190, October.

Jeffrey A. Koses, David A. Shive. 2024. “Ensuring Only Approved Software is Acquired and Used at GSA.” MEMORANDUM FOR THE GSA

ACQUISITION WORKFORCE, General Services Administration, January.

GSA, DOD, NASA. 2024. "Supply Chain Software Security." Federal Acquisition Regulation (FAR); FAR Case 2023-002, Spring.

GSA, DOD, NASA. 2024. Federal Acquisition Regulation (FAR) Case 2023-002, Supply Chain Software Security (Spring 2024)

SwA Working Group. 2024. "Software Acquisition Guide for Government Enterprise Consumers: Software Assurance in the Cyber-Supply Chain Risk Management (C-SCRM) Lifecycle.", CSCC, CISA, IT SCC, August.

김상배, 유지연 외. 2022. "한국형 경제안보 전략보고서: 이슈와 대응.", 경제·인문사회연구회, 95-103.

기획재정부. 2024. '공급망 안정화 위원회 구성 및 운영계획', 관계부처 합동, 6월.

Enduring Security Framework (ESF). 2023. "Securing the SW Supply Chain: Recommended Practices for SBOM Consumption.", ODNI, NSA CCC, CISA, CSCC, National Defense ISAC, IT SCC, November.

Michele Sandiford. 2023. "State Department takes first crack at implementing supply chain risk management tools for contracts.", Federal News Network (October 24).

박춘식. 2023. "「사이버공격의 책임은 벤더에게 있다」라고 하는 미국 정부의 주장은 올바른가?." Cybersecurity Dive 편역, 6월.

국정원, 과기정통부, 디플정위. 2024. "소프트웨어 공급망 보안 가이드라인 V1.0.", 5월.

김영명. 2024. "과기정통부 2025년 예산 19조원... 'SW 공급망 보안 관리'에 60억원 신규 편성.", 『보안뉴스』 (8월 28일).

Digital Supply Chain Security Risks and Management Implications:

A Study of the SW Acquisition Improvement Flow in the U.S. EO-14028

Yunseong Choi | Korea University

Today, supply chain cybersecurity is intertwined with economic and national security. Great power rivalries and geopolitical tensions are further complicating the supply chain landscape, making it a global issue that no single country can solve alone.

This study examines broad trends in supply chain cybersecurity policy, focusing on the implementation of the 2021 Biden Administration's Executive Order (EO-14028) and White House Office of Management and Budget memorandum (M-22-18) to 'Enhancing the Security of the Software Supply Chain through Secure Software Development Practices'

The reason for conducting a study of policy trends in major countries in times of upheaval is to identify the optimal time to adopt favorable policies and technologies, and to examine how we can apply rapidly evolving cybersecurity regulations and systems, especially EO-14028, to our own country.

This article analyzes various current U.S. strategies, policies, legal frameworks, and guidelines. In particular, it analyzes global supply chain cybersecurity incident cases to build a foundation of practical knowledge for a domestic SW supply chain risk management system and to present ideas for basic policy planning.

Keyword Digital Supply Chain, Economic Security, Risk Management, Self-attestation, SBOM