법무법인(유) 화우
YOON & YANG

LEGAL UPDATE
정보보호센터
Mar. 2023

SBOM 정책과 오픈소스 라이선스 컴플라이언스

- SBOM 도입 논의와 함께 오픈소스 라이선스 컴플라이언스 중요성도 덩달아 높아질 것 -

국가 사이버보안 위협에 대한 대응 방안 중 하나인 '소프트웨어 공급망 보안' 강화를 위해 각 국에서 'SBOM(Software Bill of Materials)' 도입에 박차를 가하고 있습니다. 우리나라도 정부가 주도하는 포럼에서 가이드라인(안내서)을 배포하여 'SBOM' 도입을 본격적으로 논의할 것으로 보입니다. 오픈소스 라이선스 컴플라이언스의 체계적인 관리 및 보안 취약점 대응을 위하여 이미 'SBOM' 도입안이 거론되고 있기도 합니다. SBOM은 소프트웨어 공급망 보안 강화뿐만 아니라 오픈소스 라이선스 컴플라이언스 달성을 위한 효과적인 도구로 평가 받고 있습니다. 이번 뉴스레터에서는 SBOM 도입 정책 배경, 현황과 향후 전망, 시사점을 살펴보도록 하겠습니다.

I. 배경

최근 솔라윈즈 해킹, 오픈소스 소프트웨어 Log4j 취약점 노출과 같이 전세계적으로 배포되어 범용적으로 사용되는 소프트웨어의 보안 위협이 대두되고 난 이후 국가 사이버보안 차원에서 '소프트웨어 공급망 보안' 강화에 대한 필요성이 급격히 높아졌습니다. 각 국은 '소프트웨어 공급망 보안'을 위한 수단을 강구하였고, 그 중 가장 적극적으로 도입이 검토되고 있는 수단이 'SBOM'입니다.

미국은 2021. 5. 12. 바이든 행정부 행정명령(EO 14028)(2021)을 필두로 연방 정부 차원에서 'SBOM' 도입을 제도화하는 방안을 적극적으로 검토하고 있고 특정 분야를 시작으로 실증 사업에도 착수하였습니다. 일본은 경제산업성 산하에 전담 TF를 조직하여 SBOM 정책 추진 방안 마련과 함께 SBOM 활용 촉진을 위한 실증사업을 추진하고 있습니다. 유럽, 중국 등 주요 국가에서도 SBOM 도입을 위한 논의에 이미 착수하였고, 소프트웨어 공급망 보안을 위하여 SBOM 도입을 제도화하는 안이 제시되고 있습니다.

우리나라도 2022. 10. 26. 과학기술정보통신부와 한국인터넷진흥원이 주축이 되어 제로트러스트·공급망 보안 포럼 발족식을 개최하고, 사이버보안 위협 대응을 위한 방안들 중에서 소프트웨어 공급망 보안 강화를 위한 SBOM 도입이 중요한 안건 중 하나로 논의 중에 있습니다. 논의의 결과로 사이버보안 위협 대응을 위한 안내서를 제작하여 배포할 예정인데, 해당 안내서에는 SBOM 도입과 관련된 정책 방향이 제시될 것으로 보입니다.

II. SBOM 도입 정책 현황과 향후 전망

가. 소프트웨어 공급망 보안 강화를 위한 각 국의 SBOM 도입 정책 현황

소프트웨어 공급망 위협은 2020. 12. 솔라윈즈 소프트웨어에 대한 해킹 사실이 드러나면서 그 심각성이 두드러졌습니다. 여러 민간 기업뿐만 아니라 정부기관까지 포함하여 업계 내에서 널리 사용되어 온 네트워크 관리 소프트웨어의 업데이트 파일에서 악성코드가 발견되었고, 통상적인 업데이트 과정으로 악성코드가 널리 퍼질 수 있다는 사실이 밝혀졌습니다. 소프트웨어 공급망을 통한 사이버 보안 위협의 노출 범위가 극도로 높아질 수 있음을 절감하게 되었습니다.

이후 2021. 11. 오픈소스 소프트웨어 Log4j의 보안상 취약점이 드러나면서 해당 소프트웨어를 이용하여 서비스를 구현한 업계에서는 서둘러 보안 패치를 적용하느라 비상이 걸린 바 있습니다. Log4j는 게임, 클라우드, 보안 서비스를 제공하는 업체들이 자신의 서비스 내 특정 기능 구현을 목적으로 범용적으로 사용하던 오픈소스 소프트웨어였기 때문에, Log4j의 보안 취약점 노출은 소프트웨어 공급망 위협으로 이어져 자칫 피해 규모가 크게 확산될 수도 있었습니다.

이제 '소프트웨어 공급망 보안' 강화는 국가 사이버보안 대응 안건으로 논의되고, 미국을 포함한 주요 국가는 소프트웨어 공급망 보안 강화를 구체적으로 실현할 수 있는 방안으로 'SBOM 도입'을 본격적으로 검토하고 있습니다. SBOM은 식품 포장지에 표시된 함량 정보와 유사하게 소프트웨어를 구성하는 요소들의 정보를 나열 정리한 일종의 자재 명세서(Bill of Material)입니다.

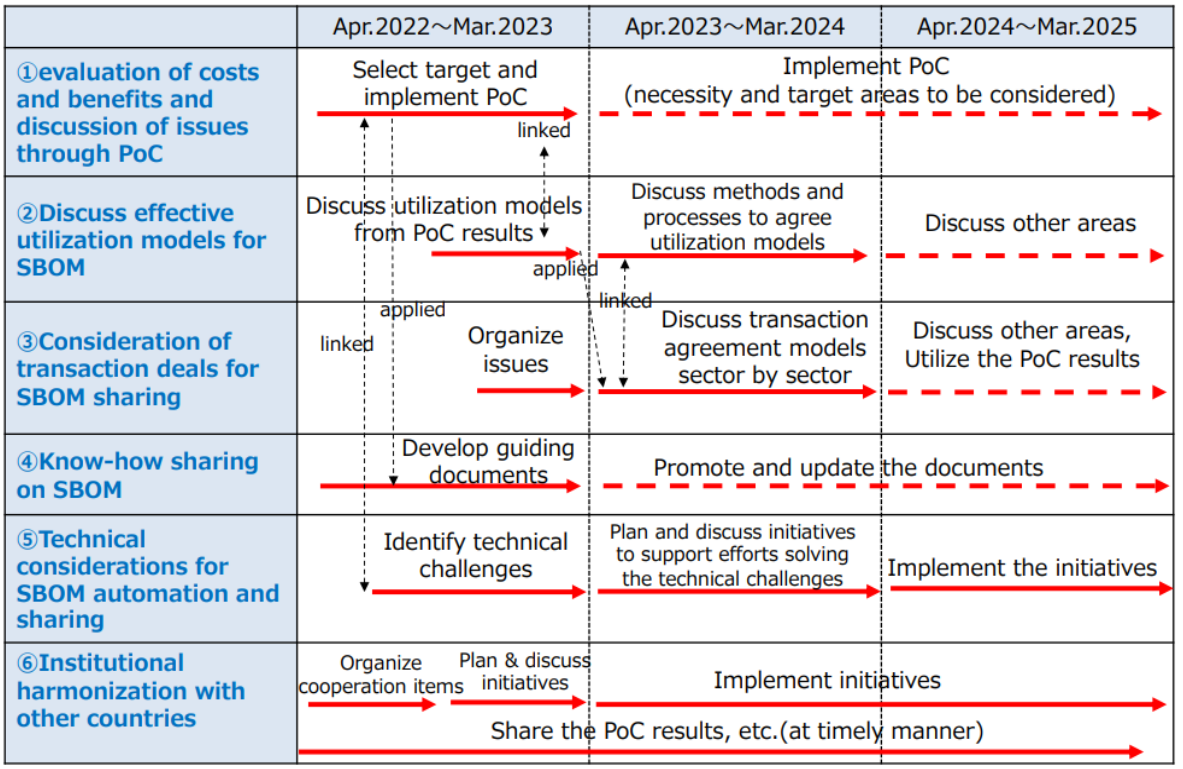
SBOM을 통하여 소프트웨어 구성요소를 파악함으로써 불시에 발생할 수 있는 보안 취약점에 신속하게 대응할 수 있습니다. 소프트웨어 공급자의 관리에만 의존하던 수준을 넘어서서, 소프트웨어 구매자도 보안 취약점 및 라이선스 분석을 수행하면서 해당 소프트웨어의 위험 요소를 평가할 수 있고, 소프트웨어를 운용하는 자도 새롭게 발견되는 취약점의 잠재적인 위험 여부를 쉽고 빠르게 판단할 수 있습니다. 종합적으로 SBOM은 소프트웨어 공급망에 놓인 여러 당사자들이 위협 요소를 파악하고 보안 취약점에 대응할 수 있어, 소프트웨어 공급망 보안 강화를 위한 효과적인 수단으로 평가받고 있습니다.

미국 바이든 행정부는 2021. 5. 12. 국가 사이버보안 개선을 위한 행정명령 EO14028을 개시하고, 연방 정부 내 소프트웨어 공급망 보안 강화를 위하여 '연방 조달 납품 대상 소프트웨어의 SBOM 제출' 가이드라인 발행하는 한편 SBOM의 최소 요건을 공시하기로 하였습니다{위 행정명령 4(e)(vii) 및 (f) 참조}. 행정명령에 따라 상무부 산하의 국가통신정보청(NTIA)는 2021. 7. 12. 'SBOM'의 최소 요건을 공시하였습니다. 상무부 산하의 국립표준기술연구소(NIST)는 2021. 11. 8. 'SBOM'에 대한 내용을 담은 가이드라인을 발표하면서 연방 정부 기관은 소프트웨어 공급자로부터 위 SBOM 최소 요건을 만족하는 SBOM이 제출될 수 있도록 하라는 지침을 명시하였습니다. 또한, 미국은 국가통신정보청 주도 하에 의료, 에너지 분야에서 SBOM 실증 사업을 수행하고, 2022. 민관협력의 보안정상회의를 2차례 주최하여 오픈소스 소프트웨어 업계 내 SBOM 활용 촉진 안을 논의하며, 향후 민간 영역으로도 산업 분야 별로 SBOM 도입을 제도화할 수 있는 기반을 마련하고 있습니다.

일본은 경제산업성(Ministry of Economy, Trade and Industry, METI)은 전담TF를 조직하여 2022. 5. 10. 오픈소스 소프트웨어 업계에서의 SBOM 활용 사례를 수집, 정리한 보고서를 발행하고, 2022. 8. 23. 공개된 영문 발표자료에서는 각 산업계의 노하우를 공유하기 위한 가이드라인 작성, 효과적인 활용 촉진을 위한 실증사업 수행 계획 포함한 SBOM 정책 로드맵을 제시하였습니다. 한편, 일본 경제산업성은 오픈소스 기관

및 민간 기업들과 함께한 2022 Open Source Security Summit에서 위와 같은 성과와 계획을 제시하며 SBOM 활용 촉진의 필요성을 공감하며 향후 정책적인 노력을 계속하겠다는 전망을 밝히기도 하였습니다.

<출처: 일본 경제산업성 2022. 8. 23. 공개 영문 발표자료>



유럽연합도 2020. 사이버보안 관리가 필요한 의료기기, 사물인터넷 업계를 중심으로 보안 가이드라인을 발표하며 보안 취약점을 선별하고 관리하는 수단으로 SBOM을 제시하였고, 2022. 9. 15. 디지털 제품의 사이버보안 요건을 규정하기 위한 사이버복원력법(Cyber Resilience Act)을 입법제안하면서 보안 취약점 식별 및 관리를 위한 수단으로 SBOM이 거듭 제시되었습니다. 예컨대, 디지털 제품에 대해 SBOM 정보를 열람할 수 있도록 하고, 제품의 기술문서에는 SBOM 정보가 제시되도록 하는 규정이 포함되었습니다.

중국은 2021. 공업정보화부 산하의 정보통신연구원(CAICT)이 소프트웨어 공급망 보안 백서를 발간하고 보안 취약점에 대응할 수 있는 수단으로 SBOM을 제시하는 한편, 2022. 구체적인 작성법이나 활용방안을 담은 실무가이드를 발간하며 주요 국가들의 SBOM 정책 방향에 발맞추어 가고 있습니다.

우리나라는 2022. 10. 26. 과학기술정보통신부와 한국인터넷진흥원이 주축이 되어 제로트러스트·공급망 보안 포럼 발족식을 개최하고, 소프트웨어 공급망 보안 부문의 정책, 산업 방향을 제시하는 분과에서 SBOM 도입에 대한 논의를 진행하고 있습니다{아래 포럼 분과 구성(안) 참조}. 제로트러스트·공급망 포럼은 2023. 1분기 내에 국내 산업 보안에 적용될 제로트러스트 안내서를 발간할 예정이며, 공급망 포럼의 논의 내용을 반영하여 SBOM 도입 정책 방향에 대한 내용도 포함될 것으로 전망되고 있습니다. 또한, 2023. 부터 의료 산업 등의 일부 산업계를 중심으로 SBOM 실증 사업을 진행할 계획도 세우고, 실증 추진을 위한 민관협의회도 구성할 예정이라고 합니다(바이라인네트워크, '제로트러스트' 가이드라인 늦어진다...내년 2월 나올 듯, 2022. 12. 8.).

나. 오픈소스 라이선스 컴플라이언스 목적의 SBOM

사실, 앞서 살펴본 바와 같이 미국을 포함한 주요 국가에서는 소프트웨어 공급망 보안 강화를 목적으로 한 SBOM 도입이 논의되었으나, 오픈소스 소프트웨어 업계에서 '소프트웨어 구성요소의 체계적 관리' 필요성은 이미 업계 내에서 널리 공감하고 있는 안건이었습니다. 소프트웨어를 구성하는 요소들의 보안 취약점을 식별하고 관리한다는 목적 이외에 '오픈소스 라이선스 컴플라이언스'를 위해서 SBOM과 같은 목록 체계가 필요했기 때문입니다.

일반적으로 소프트웨어를 개발하는 경우 각기 다른 기능과 목적을 따르는 더 작은 단위의 소프트웨어를 조합하고 연동하여 구현합니다. 오픈소스 소프트웨어 업계에는 그 작은 단위의 소프트웨어들이 방대한 규모로 축적되어 있고, 특정 기능을 구현하기 위하여 처음부터 새로 소스코드를 작성할 필요 없이 누군가가 이미 같은 목적으로 만들고 공개한 소프트웨어를 자유로이 활용할 수 있습니다. 다만, 오픈소스 소프트웨어는 특정 의무를 규정한 라이선스를 준수하여 사용하여야 합니다. 통상 라이선스 유형은 정형화되어 있습니다.

다수의 오픈소스 소프트웨어를 사용하여 제품화 하거나 인터넷 서비스를 준비하는 경우, 그 제품이나 서비스를 구성하는 오픈소스 소프트웨어의 라이선스 간에 서로 충돌되는 사항은 없는지, 각 오픈소스 소프트웨어의 라이선스가 요구하는 의무사항과 사업 방향에 배치되는 사항은 없는지를 살펴보아야 합니다. 라이선스 의무사항 준수 여부는 저작권 침해 여부가 문제되거나 회사 내 자산인 소스코드를 강제로 공개해야 하는 문제로 이어질 수 있기 때문에, 소프트웨어 개발 전(全) 단계에 걸친 오픈소스 라이선스 컴플라이언스 정책을 수립하여 소프트웨어를 구성하는 오픈소스 소프트웨어 요소들을 체계적으로 검증하고 관리하여야 합니다. 오픈소스 소프트웨어 업계에서 SBOM은 오픈소스 라이선스 컴플라이언스 입장에서 보더라도 효과적인 수단으로 평가 받고 있습니다.

다만, SBOM이 오픈소스 라이선스 컴플라이언스 목적으로 도입된 사례는 많지 않습니다. SBOM은 오픈소스 라이선스 컴플라이언스를 위한 의무적인 수단은 아니고, 오픈소스 소프트웨어를 누구나 자유롭게 쓸 수 있다는 인식만 널리 퍼져있을 뿐, 오픈소스 라이선스 컴플라이언스에 대한 중요성까지 업계 전반에 자리잡았다고 볼 수는 없었기 때문입니다. 소프트웨어 공급망 보안에 대한 인식이 제고되기 전에는, 소프트웨어를 공급 받는 입장에서 그 소프트웨어를 구성하는 요소까지 알 필요는 없었기 때문에, 소프트웨어 공급자가 자발적으로 오픈소스 라이선스 컴플라이언스를 사업 운영의 중요한 과제로 삼지

않는 이상 SBOM과 같은 목록 체계를 관리할 필요가 적었습니다. 이에 오픈소스 라이선스 컴플라이언스 정책상 필요에 따라 SBOM 도입을 적극적으로 검토하여야 한다는 인식에까지 이르지는 않는 경우가 대다수였습니다.

다. SBOM 도입 정책 추진에 따른 향후 전망

SBOM은 소프트웨어 공급자의 편의 수단을 넘어서서 국가 사이버보안 대응 차원에서 소프트웨어 공급망 보안 강화 수단으로 거론되고 있고, 소프트웨어 공급자가 자발적으로 생성하는 내부 관리 체계 수단을 넘어서서 적어도 소프트웨어를 공급받거나 이를 운용하는 당사자를 포함하는 광범위한 주체들이 함께 관리하고 추적하는 대상이 될 가능성이 높습니다. SBOM을 접근할 수 있는 대상이 소프트웨어 공급자 외부로까지 확대된다면, 오픈소스 라이선스의 준수 여부가 이슈화 될 가능성이 높아질 것이므로, 오픈소스 라이선스 컴플라이언스 관리의 필요성이 높아질 수 밖에 없습니다.

오픈소스 소프트웨어 업계의 대표 주자인 리눅스재단은 2022. 1. 보고서에서 소프트웨어 공급망 보안 강화를 위하여 거론되고 있는 SBOM 도입으로 오픈소스 라이선스 컴플라이언스 관리도 함께 용이해지는 혜택을 볼 것이라는 설문조사 결과를 내놓았습니다. 오픈소스 소프트웨어 업계에서 SBOM은 국가 사이버보안 대응 차원에서 최우선 과제인 소프트웨어 공급망 보안 강화를 달성할 수 있는 수단임과 동시에 오픈소스 라이선스 컴플라이언스까지 점검할 수 있는 도구로 인식되고 있음을 보여줍니다. 오픈소스 소프트웨어 업계의 주도 하에 SBOM 정책으로 소프트웨어 공급망 보안 강화하겠다는 과업에 더하여 오픈소스 라이선스 컴플라언스의 중요성 또한 부각될 것이라 예상됩니다.

III. 시사점

미국 바이든 행정부를 필두로 소프트웨어 공급망 보안 강화를 위한 SBOM 도입 정책은 대세적인 흐름이 되고 있고, 일본, 유럽연합, 중국을 포함한 주요 국가에서는 실증사업, 입법제안을 추진하며 소프트웨어 공급망 보안 강화를 위한 SBOM의 제도화 기반을 마련하고 있습니다. 디지서트(digicert)는2023. 사이버보안 전망으로 내세운 8가지 항목을 발표하였고, 그 중 하나로 소프트웨어 공급망 보안 강화를 위하여 SBOM의 해가 될 것이라는 내용이 포함되어 있습니다.

우리나라도 다른 주요 국가들의 정책 흐름에 발 맞추어 SBOM 도입 논의가 활발하게 이루어질 예정이고, 제로트러스트·공급망 보안 포럼에서 발간할 안내서를 통해 향후 정책 방향의 밑그림이 그려질 것이라 보입니다.

현재의 SBOM 도입에 대한 논의는 우선적으로 소프트웨어 공급망 보안 강화에 초점이 맞춰질 것입니다. 그러나 SBOM도입 정책으로 단지 소프트웨어 공급망 보안 이슈만 다루는데 그치지 않을 것이라 보입니다. SBOM 정책 추진으로 발생할 효과나 SBOM으로 오픈소스 라이선스 컴플라이언스도 달성할 수 있다는 특징을 고려해 보면 SBOM 도입에 대한 논의는 오픈소스 라이선스 컴플라이언스에 대한 논의로 이어질 것이라 예상해 볼 수 있습니다. 두 가지 관점을 염두에 두고 SBOM 정책에 대한 논의를 지켜볼 필요가 있습니다. 향후 SBOM 도입 논의에 대한 동향을 지속 추적하면서 뉴스레터를 통해 관련 내용을 업데이트 해드리겠습니다.

화우의 정보보호센터는 오랜 경험과 축적된 노하우를 기반으로 기업 고객을 위한 최적의 솔루션을 안내해 드리고 있습니다. 정보보호 관련 법령의 해석 및 그 대응과 정보보호 기술적 자문(해킹 진단, 보안취약점) 등 포괄적인 올인원(All-in-One) 서비스를 제공하고 있습니다. 관련하여 문의사항이 있으신 경우 언제든지 화우에 연락하여 주시기 바랍니다.

Contacts

이광욱
파트너변호사
T. (+82) 2 6003 7535
E. kwlee@yoonyang.com

이근우
파트너변호사
T. (+82) 2 6003 7558
E. klee@yoonyang.com

권은구
변리사
T. (+82) 2 6182 8538
E. egkwon@yoonyang.com

백재환
전문위원
T. (+82) 2 6182 8366
E. jhb@yoonyang.com

지재원
연구위원
T. (+82) 2 6003 7568
E. jwji@yoonyang.com