IoTcube Conference 2025

- Archimedes International Healthcare Security Week -

환자 안전과 산업 경쟁력 확보를 위한 의료기기 사이버보안과 SBOM

고려대학교 소프트웨어보안연구소
Korea University
Center for Software Security and Assurance

Archimedes Center for
Health Care and Medical Device Cybersecurity
at Northeastern University

August 26, 2025 · Seoul, South Korea

https://cssa.korea.ac.kr · https://iotcube.net

IoTcube Conference 2025

- Archimedes International Healthcare Security Week -

환자 안전과 산업 경쟁력 확보를 위한 의료기기 사이버보안과 SBOM

CONTENTS

본 보고서는 제9회 IoTcube Conference 2025를 기반으로 의료기기 사이버보안과 글로벌 공급망 보안 대응 기술(SBOM/VEX)을 정리한 결과물입니다. 과학기술정보통신부 및 정보통신기획평가원(IITP) 정보보호핵심원천기술개발사업의 지원으로 수행되었습니다.

고려대학교 소프트웨어보안연구소
(CSSA, Center for Software Security and Assurance)

고려대학교 소프트웨어보안연구소(CSSA, Center for Software Security & Assurance, 소장 이희조 교수)는 소프트웨어 공급망 보안과 취약점 자동 분석 기술을 선도하는 글로벌 연구 허브입니다.

2015년 과학기술정보통신부의 지원으로 설립된 'IoT 소프트웨어보안 국제공동연구센터'를 전신으로 하며, 미국 카네기멜론대·영국 옥스퍼드대·스위스 ETH Zurich 등 세계 유수 연구기관과 협력해

2016년 **보안취약점 자동분석 플랫폼 IoTcube.net**을 개발·공개하고,
2017년부터 매년 **IoTcube Conference를 개최**하며 기술 확산에 기여해왔습니다.

이희조 교수는 2010년 카네기멜론대 방문연구 당시, 보안 취약점 자동분석 연구 가능성에 주목해 누구나 쉽게 사용할 수 있는 오픈소스 소프트웨어 취약점 탐지, 컴포넌트 분석 및 의존성 추적 도구 연구를 시작했습니다.

연구소는 글로벌 공급망 보안의 핵심 의제로 떠오른 SBOM(Software Bill of Materials) 및 VEX(Vulnerability Exploitability eXchange) 기술 개발에 집중하고 있으며, Centris (ICSE '21), Vuddy (IEEE S&P '17), Cneps (ICSE '24) 등 오픈소스 보안 핵심 기술을 개발해 국제 규제 대응과 산학 협력에 적극 활용하고 있습니다.

2023년 8월에는 **국내 최초 공개형 SBOM 도구 Hatbom**을 IoTcube.net에 런칭하여 한국정보보호산업협회(KISIA)와 기업 실증을 진행하고, 기술 검증과 함께 민간 기업의 SBOM 준비를 위한 참고 자료를 제공했습니다.

2018년에는 산업계 전문 활용을 위해 **고려대 기술지주 자회사 ㈜래브라도랩스**를 설립하여 오픈소스 보안 및 SBOM 관리 솔루션 Labrador를 의료·자동차·금융 등 산업 현장에 공급하고 해외 사업도 확장하고 있습니다.

연구소는 기술 연구와 더불어 2019년 고려대 융합보안대학원(일반대학원 컴퓨터학과 컴퓨터보안전공)을 설립하여 차세대 보안 인재 양성과 산·학·연·관 생태계 구축에 힘쓰고 있으며, 2024년부터는 ETH Zurich·조지아텍·노스이스턴대학과 함께 SBOM 및 VEX 자동 검증 국제공동연구를 수행 중입니다.

본 보고서는 2025년 8월 26일, 미국 노스이스턴대학교 산하 Archimedes Center for Healthcare and Medical Device Cybersecurity와 공동으로 개최한 제9회 IoTcube 국제 컨퍼런스의 의료기기 사이버보안 논의와 글로벌 공급망 보안 기술을 정리한 자료입니다.

[주요 링크]
- 연구소 홈페이지: https://cssa.korea.ac.kr
- 고려대 CCS Lab(Computer&Communication Security Lab): https://ccs.korea.ac.kr/
- 보안 취약점 자동분석 플랫폼 아이오티큐브(IoTcube): https://iotcube.net
- 기업용 솔루션 래브라도랩스: https://labradorlabs.ai

고려대 CSSA | IoTCube.net | 래브라도랩스

들어가며

의료기기는 환자 생명과 직결되는 핵심 장치이자, 병원·지역사회까지 연결되는 디지털 생태계의 한 축이다. 최근 의료기관을 겨냥한 사이버 공격은 단순한 정보 유출을 넘어 치료 지연, 장비 오작동, 심지어 환자 생존율 저하로까지 이어지고 있다. 응급의료 전문가들은 랜섬웨어가 심정지 환자의 생존율을 급격히 낮추는 임상 데이터를 제시했고, 심장 박동기·제세동기, 인슐린 펌프 해킹 등 실험적 입증은 의료기기 보안이 더 이상 가상의 위협이 아님을 보여주었다.

이러한 위기 속에서 세계 각국은 규제 대응을 본격화하고 있다. 미국은 대통령 행정명령과 식품의약국(FDA) 지침을 통해 SBOM(Software Bill of Materials) 제출을 법제화했고, 유럽연합도 사이버 복원력법(Cyber Resilience Act, CRA)을 통해 디지털 제품 전반의 보안을 강화하고 있다. 대한민국 역시 SBOM·VEX 기반 공급망 보안 연구와 의료기기 보안 제도화를 본격화하기 시작했으며, 국제 협력과 정책 논의를 가속화해 선도적 역할을 확보할 기회가 열리고 있다.

본 보고서는 2025년 8월 26일, 고려대학교 소프트웨어보안연구소(CSSA)와 미국 노스이스턴대학교 Archimedes Center for Healthcare and Medical Device Cybersecurity가 공동 개최한 IoTcube Conference 2025에서 논의된 의료기기 사이버보안 최신 동향과 글로벌 공급망 보안 대응 기술을 정리한 것이다. 특히 SBOM과 VEX(Vulnerability Exploitability eXchange) 기술을 중심으로 환자 안전을 보장하고 의료 산업의 국제 경쟁력을 강화하기 위한 정책·기술적 과제를 제시한다.

IoTcube Conference 2025 포스터와 행사 사진

1. 급증하는 의료기관 사이버 위협

케빈 푸(Kevin Fu)는 미국 보스턴에 위치한 노스이스턴대학교 전기·컴퓨터공학과, Khoury 컴퓨터과학대학, 바이오공학과 교수로, 의료기기 사이버보안 연구소인 Archimedes Center for Healthcare and Medical Device Cybersecurity를 이끌고 있다.


Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses

2008

Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses (IEEE S&P 2008): 의료기기 해킹이 실제 환자 생명을 위협할 수 있음을 실험적으로 입증한 기념비적 연구

현대 의료기관은 전자의무기록(EHR), 환자 모니터링 장비, 수술 로봇, 약물 주입기 등 디지털 인프라에 폭넓게 의존한다. 그만큼 사이버 공격이 환자 치료와 안전에 미치는 영향도 커지고 있으며, 진료 지연과 생명 위협, 병원 운영 차질, 산업 신뢰 손실로 이어질 수 있다.

1.1. 의료기기 보안 위협의 역사적 사례

노스이스턴대 **케빈 푸(Kevin Fu)** 교수(前 미국 식품의약국(FDA) 의료기기 보안 책임자)는 의료기기 사이버 위협의 전개를 돌아보며 환자 안전에 실질적으로 영향을 미친 대표 사례들을 소개했다.

- **심장박동기·제세동기 취약점(2006-2008):** 암호화되지 않은 이식형 심장박동기를 소프트웨어 정의 무선(SDR)으로 해킹해 부정맥을 유발할 수 있음을 세계 최초 실험적 입증. 케빈 푸 교수팀의 본 연구(IEEE S&P 2008)는 미국 회계감사원(GAO)이 FDA에 보안 강화 필요성을 공식 권고하는 계기로 작용
- **인슐린 펌프 해킹 시연(2011):** 화이트해커 버나비 잭(Barnaby Jack)이 세계적 해킹 컨퍼런스 Black Hat에서 수백 피트 거리 떨어진 인슐린 펌프를 원격 조종해 과다 투여 가능성을 공개, 의료기기 무선 보안 취약성에 경각심 제고
- **Hospira Symbiq 주입기 취약점(2015):** 기본 비밀번호 노출과 네트워크 보안 미비로 원격 조작 가능성이 보고되자, 미국 FDA는 해당 모델 사용 중단을 권고. 사이버보안 문제로 FDA가 제품 사용중단을 직접 권고한 대표적 사례로, 의료기기 안전성 평가에 보안이 본격 반영되는 전환점
- **GE Healthcare 기본 비밀번호 사건(2020):** 수십 종의 GE 의료영상 장비에서 하드코딩된 기본 비밀번호가 발견되자, CISA와 FDA가 보안 패치와 설정 변경을 권고, 이후 기본 비밀번호 제거가 의료기기 설계 가이드라인에 반영

푸 교수는 의료기기 보안을 “1840년대 의사들의 손 씻기 논쟁”에 비유하며, 보안은 선택이 아니라 환자 생명을 지키기 위한 필수 조건이라고 강조했다.

1.2. 네트워크로 확장된 병원의 공격 표면

미국 최상위 의료기관인 미시간 메디슨 **잭 쿠팔(Jack Kufahl)** 최고보안책임자(CISO)는 현대 병원의 디지털화가 가져온 공격 표면의 급격한 확장을 경고했다.

오늘날 병원은 전자의무기록(EHR), 환자 모니터링 장비, 수술 로봇, 약물 주입기, 스마트 병상, 심지어 출입문·엘리베이터·조명까지 대부분의 운영이 네트워크로 연결돼 있다. 환자 치료 역시 가정·학교·지역사회까지 확장되며 공격 경로는 사실상 무한대로 넓어지고 있다.

잭 쿠팔(Jack Kufahl)은 미국 미시간 대학교 소속 미시간 메디슨(Michigan Medicine) 최고정보보호책임자(CISO)로, 20년 이상 정보기술 경력을 보유하고 있다.

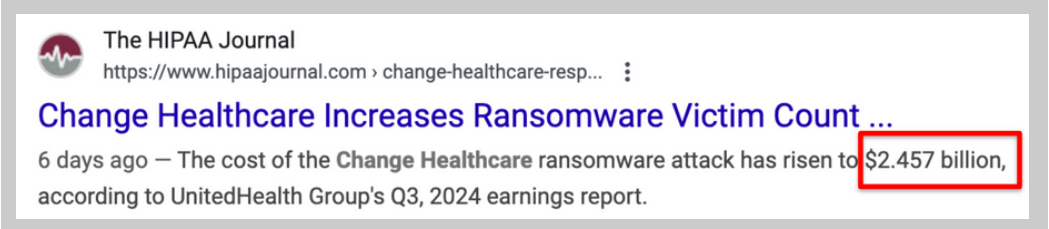
미시간 메디슨은 연구, 환자 진료, 교육 분야에서 세계적 권위를 인정받는 미국 최고의 학술 의료기관 중 하나다.

실제 미시간 메디슨에서는 뇌 수술용 레이저 장비가 인터넷에 노출되고, 제조사 매뉴얼에 기록된 기본 비밀번호만으로 누구나 접근할 수 있었던 사례가 보고됐다. 이처럼 생명과 직결된 장비가 보호되지 않은 채 연결돼 있는 경우는 여전히 빈번하다.

쿠팔 CISO는 병원이 직면한 주요 위협으로 ▲표적형 랜섬웨어와 이중 갈취(Double Extortion), ▲공급망 공격, ▲AI 기반 자동화 공격, ▲데이터 유출 및 내부자 리스크를 지적했다. 이와 함께 지원 종료된 레거시 장비, 네트워크 분리의 어려움, 보안·데이터·임상 지식을 모두 갖춘 인력 부족이 병원 보안을 더욱 복잡하게 만든다고 설명했다.

그는 “보안은 기술이나 예산만으로 해결되지 않는다”며 ▲의료진·IT·보안팀 간 지속적 협력 구조 구축, ▲환자 안전에 직결되는 핵심 위협 중심의 위협 인텔리전스 체계 확립의 필요성을 강조했다.

또한 2024년 미국 체인지 헬스케어(Change Healthcare) 대규모 랜섬웨어 공격으로 수천 개 병원의 청구·지불 업무가 마비된 사례를 언급하며, 단일 장애 지점(SPoF)이 의료 생태계 전체를 위기에 빠뜨릴 수 있다고 경고했다.



2024년 병원결제플랫폼 ‘체인지 헬스케어(Change Healthcare)’ 랜섬웨어 공격으로, 관련 서비스를 사용하던 병원까지 혼란에 빠졌다.
출처: https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack

1.3. 환자 생존율에 영향을 미친 랜섬웨어 공격

크리스천 다메프(Christian Dameff)는 미국 캘리포니아대 샌디에이고(UC San Diego, UCSD) 의과대학 응급의학과·컴퓨터공학과 조교수이자 UCSD Center for Healthcare Cybersecurity 공동 책임자이다.

Open capture the flag champion 우승 경력의 해커이자 응급의학 전문의로, 임상과 보안을 연결하는 연구를 주도하고 있다.


BRIEF REPORT

OPEN

Ransomware Cyberattack Associated With Cardiac Arrest Incidence and Outcomes at Untargeted, Adjacent Hospitals

Thaidan T. Pham, MD[1]
Theoren M. Loo, MS[2]
Atul Malhotra, MD[3]
Christopher A. Longhurst, MD, MS[3,4]
Diana Hylton, MD[3]
Christian Dameff, MD, MS[3,4]
Jeffrey Tully, MD[3]
Gabriel Wardi, MD, MPH[3,4]
Rebecca E. Sell, MD[3]
Alex K. Pearce, MD[3]

OBJECTIVES: Healthcare ransomware cyberattacks have been associated with major regional hospital disruptions, but data reporting patient-oriented outcomes in critical conditions such as cardiac arrest (CA) are limited. This study examined the CA incidence and outcomes of untargeted hospitals adjacent to a ransomware-infected healthcare delivery organization (HDO).

DESIGN, SETTING, AND PATIENTS: This cohort study compared the CA incidence and outcomes of two untargeted academic hospitals adjacent to an HDO under a ransomware cyberattack during the pre-attack (April 3–30, 2021), attack (May 1–28, 2021), and post-attack (May 29, 2021–June 25, 2021) phases.

INTERVENTIONS: None.

MEASUREMENTS AND MAIN RESULTS: Emergency department and hospital mean daily census, number of CAs, mean daily CA incidence per 1,000 admissions, return of spontaneous circulation, survival to discharge, and survival with favorable neurologic outcome were measured. The study evaluated 78 total CAs: 44 out-of-hospital CAs (OHCAs) and 34 in-hospital CAs. The number of total CAs increased from the pre-attack to attack phase (21 vs. 38; $p = 0.03$), followed by a decrease in the post-attack phase (38 vs. 19; $p = 0.01$). The number of total CAs exceeded the cyberattack month forecast (May 2021: 41 observed vs. 27 forecasted cases; 95% CI, 17.0–37.4). OHCA cases also exceeded the forecast (May 2021: 24 observed vs. 12 forecasted cases; 95% CI, 8.0–18.8). Survival with favorable neurologic outcome rates for all CAs decreased, driven by increases in OHCA mortality: survival with favorable neurologic rates for OHCAs decreased from the pre-attack phase to attack phase (40.0% vs. 4.5%; $p = 0.02$) followed by an increase in the post-attack phase (4.5% vs. 41.2%; $p = 0.01$).

CONCLUSIONS: Untargeted hospitals adjacent to ransomware-infected HDOs may see worse outcomes for patients suffering from OHCA. These findings highlight the critical need for cybersecurity disaster planning and resiliency.

KEYWORDS: cardiac arrest; cardiac arrest; cybersecurity; ransomware; cyberattack; outcomes

Ransomware cyberattacks on healthcare delivery organizations (HDOs) are increasing in frequency and sophistication (1). Ransomware is a type of malicious software that can block access to computer systems and networks until a ransom is paid. In a clinical environment dependent on connected technology, ransomware may disrupt patient care workflows (2). On May 1, 2021, a four-hospital HDO was "infected" by a ransomware cyberattack, resulting in the loss of electronic medical records and systems for one month (3). Although the operational effects of ransomware-infected HDOs have been reported, there are limited data regarding how ransomware cyberattacks impact adjacent, untargeted hospitals (4). To our knowledge, Dameff et al (5) was the first study patient outcomes in neighboring, untargeted hospitals and found

Copyright © 2024 The Authors. Published by Wolters Kluwer Health, Inc. on behalf of the Society of Critical Care Medicine. This is an open-access article distributed under the terms of the Creative Commons Attribution-Non Commercial-No Derivatives License 4.0 (CCBY-NC-ND), where it is permissible to download and share the work provided it is properly cited. The work cannot be changed in any way or used commercially without permission from the journal.

DOI: 10.1097/CCE.0000000000001079

Critical Care Explorations www.ccejournal.org 1

Pham, Christian Dameff, Jeff Tully 등의 연구 「Ransomware Cyberattack Associated With Cardiac Arrest Outcomes」(2024)에 따르면, 랜섬웨어 공격 당시 인근 병원으로 이송된 OHCA(심정지) 환자의 신경학적 정상 생존율이 평소 약 40%에서 4.5%로 급감했다.

응급의학 전문의이자 화이트 해커인 **크리스천 다메프(Christian Dameff)** UC 샌디에이고(UCSD) 교수는 "랜섬웨어는 단순한 IT 장애가 아니라 환자 생존율을 급격히 낮춘다"고 경고했다.

UCSD 연구팀은 2021년 샌디에이고 지역에서 실제로 발생한 대형 랜섬웨어 공격 사례를 분석해, 공격을 받은 의료기관과 인접 비공격 병원에 이송된 심정지(out-of-hospital cardiac arrest, OHCA) 환자 데이터를 전·중·후기 3단계로 비교 분석했다.

그 결과, 공격 전 평소 OHCA 환자의 퇴원 시 신경학적으로 양호한 생존율은 약 40%였으나, 공격 기간 중 4.5%까지 급감했고, 공격 종료 후 40%대로 회복되는 양상이 관찰됐다. 또한 공격 중 전체 심정지 건수는 예측치를 크게 웃돌았으며(관찰 41건 vs 예측 27건), 특히 병원 외 심정지가 두 배 가까이 증가해(관찰 24건 vs 예측 12건) 응급의료 체계에 심각한 부담을 준 것으로 나타났다.

다메프 교수는 "보안사고가 발생하면 임상 현장은 전자의무기록(EHR)이나 진료 지원 시스템을 즉시 대체할 수단이 거의 없다"고 지적하며, 병원 자체의 복원력(resilience) 확보가 필수적이라고 강조한다. 이를 위해 그의 연구팀은 HR3P(Healthcare Ransomware Resiliency & Response Program)을 통해 다음과 같은 실전 대응 도구를 개발하고 있다.

- **CRASHCART:** 네트워크 마비 시 최소한의 진료 기능을 빠르게 복원 (현장 시연에서 39분 만에 20개 병상 응급실 가동)
- **RANSOMWHERE?:** 공격 감지 및 영향 범위 실시간 시각화
- **THE TOME:** 사이버공격 대비 임상 대응 매뉴얼

이 사례는 의료기관이 사전 대비와 복원력 구축 없이 단순 방어 위주에 머물 경우, 사이버 공격이 단순한 시스템 장애를 넘어 응급 환자의 생존율과 치료 결과를 직접 악화시킬 수 있음을 보여준다.

의료 분야 주요 사이버 위협

연도	사건	영향	시사점
2006~2008	심장박동기·제세동기 해킹 연구 (Halperin et al.)	무선 신호 조작으로 기기 기능 중단·부정맥 유발 가능	의료기기 해킹이 실제 환자 생명에 치명적 영향을 줄 수 있음을 최초 입증
2011	인슐린 펌프 해킹 (Jay Radcliffe, Barnaby Jack)	무선 통신 조작으로 인슐린 과다 투여 가능	무선 통신 보안·인증 부재가 치명적 취약점으로 작용
2015	Hospira Symbiq 주입기 취약점	원격 약물 조작 가능성 → FDA 사용 중단 권고	기본 비밀번호·허술한 네트워크 설계가 중대한 환자 위험 초래
2016	St. Jude Medical (Abbott) 심장박동기 사건	기기 임의 변경/비활성화 가능 → 리콜 발생	암호화 등 보안 테스트 부족이 산업의 신뢰성을 위협
2017	WannaCry 랜섬웨어	영국 NHS 병원 수백 곳 마비 및 진료 일정 취소	랜섬웨어 하나로 의료기관 전체 운영 마비 및 진료 차질 발생 가능
2018	Medtronic 심장 프로그래머 취약점	원격 해킹 가능성 공식 지적	임플란트 관리 소프트웨어 취약점 또한 환자 안전에 영향을 미침
2019	Urgent/11 글로벌 취약점	세계 각국 의료기기 및 임베디드 장비 다수 영향	의료기기도 글로벌 소프트웨어 취약점으로부터 자유롭지 않음
2019	Medtronic MiniMed 인슐린 펌프 리콜	취약점 노출로 대규모 리콜 발생	취약점 관리 실패 시 막대한 비용·신뢰 손실 발생
2020	GE Healthcare 의료기기 기본 비밀번호 취약점	하드코딩된 비밀번호로 누구나 장비 접근 가능	레거시 설계 관행 및 기본값 관리를 규제로 해결할 필요성 인식
2021	Elekta 방사선 치료 클라우드 시스템 랜섬웨어 공격	암 환자 치료 일정 대거 지연	클라우드 보안 취약점이 임상 현장에 직접적 피해 초래
2021	Log4j 글로벌 오픈소스 취약점	다수 의료 소프트웨어 및 장비에 광범위한 영향	오픈소스 취약점 관리 미흡 시 전체 생태계 위협 가능
2022	Illumina 유전자 분석장비 취약점	환자 데이터 변조 및 결과값 위변조 가능성	정밀 의료 데이터의 무결성과 신뢰성이 직접적으로 위협받음
2024	Change Healthcare 랜섬웨어 사건	미국 내 수천 병원 진료·청구 마비, 약 24억 달러(3조 원대) 피해 발생	3자 공급망 공격이 전체 의료 생태계 마비시킬 수 있음을 실증

(출처: Kevin Fu 교수 발표자료)

병원 최고보안책임자(CISO)가 전하는 2025년 사이버보안 위협과 대응 전략

Insights from Jack Kufahl, CISO at Michigan Medicine

1. 위협 환경의 변화

- **IoMT(Internet of Medical Things) 확산:** 약물 주입기, 심장박동기, 스마트 병상, 환자 모니터, 수술 로봇, 엘리베이터·조명·HVAC까지 병원 장비 대부분이 네트워크에 연결되며 공격 표면이 기하급수적으로 확대
- **데이터 폭증과 민감성:** 대형 병원은 연간 50PB 이상 데이터 생성, 이 중 90% 이상이 개인건강정보(PHI)로 유출 시 막대한 금전·평판 피해로 이어질 수 있음

2. 대표 공격 유형

- **표적형 랜섬웨어와 이중 갈취(Double Extortion):** 시스템 마비 + 데이터 유출 협박을 동시에 가하는 공격이 일반화
- **공급망 공격:** 협력사·외부 소프트웨어를 통한 우회 침입 증가
- **AI 기반 공격:** 자동화된 피싱·탐지 회피·취약점 발굴 등으로 공격 속도·규모 확대
- **데이터 수익화 및 내부자 리스크:** 의료정보(PHI)가 다크웹에서 고가 거래되면서, 스트레스·과로한 내부 인력이 사회공학 공격에 취약

3. 의료기기와 시스템 취약점

- **레거시 장비:** 구형 OS·지원 종료된 소프트웨어가 계속 사용 → 패치 불가
- **기본 비밀번호·노출 포트:** MRI, 인공호흡기, 인슐린 펌프 등에서 공통 발견
- **업데이트 부재:** 제조사 지원이 끊겨도 계속 사용되는 '좀비 장비(zombie tech)'

4. 대응 전략

- **망분리(Segmentation):** 중요 장비별 네트워크 분리해 감염 확산 방지
- **정기 패치 & 테스트:** 임상 검증팀·보안팀 협력, 테스트-수정-배포 주기 관리
- **강력 인증:** 기본 비밀번호 제거, 다중 인증(MFA), 기기 인증서 적용
- **상시 모니터링:** 연 1회 점검이 아닌 지속적 취약점 관리 체계
- **사전 모의훈련:** EHR·생명유지장치 공격 시나리오 대비

잭 쿠팔(Jack Kufahl, 미시간 메디슨 CISO)

2. 의료기기 사이버보안의 필요성 및 글로벌 규제

2.1. 미국 등 해외 사례: 단계적 고도화 및 법제화

미국의 의료기기 사이버보안 규제는 학계의 취약점 경고에서 출발해, 실제 해킹 사례와 정부 권고, FDA 가이드라인을 거쳐 법제화까지 단계적으로 고도화돼 왔다.

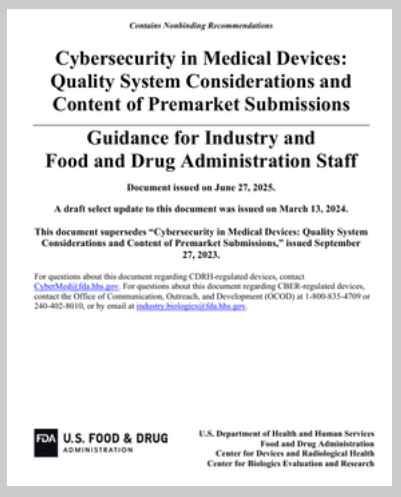
2006~2008년 케빈 푸 연구팀의 이식형 심장박동기·제세동기 무선 취약점 연구가 논의를 촉발했고, 2010년대에는 인슐린 펌프·약물 주입기 등 실제 해킹 사례가 공개되며 환자 안전 리스크가 구체화되었다.

2012년 미국 회계감사원(GAO)과 국립표준기술연구소(NIST)가 의료기기 사이버보안 가이드라인 부재를 공식 지적했고, 2014년 미국 식품의약국(FDA)은 의료기기 사이버보안 관련 최초의 사전승인(pre-market) 가이드라인을 발표해 보안 기준 마련에 나섰다.

2022년 미국 의회는「연방지출법(Consolidated Appropriations Act, 2023)」을 통해 연방 식품·의약·화장품법(FD&C Act)에 Section 524B를 신설, 의료기기 사이버보안을 법적 의무로 규정하였다. 이에 따라 2023년 3월 29일 이후 미국 내 접수되는 '사이버 디바이스' 신규 허가 신청에는 다음이 요구된다.

- **사이버보안 엔지니어링 계획:** 취약점 관리, 위험 허용 기준, 사고 대응 절차 등을 FDA 사전 제출
- **SBOM:** 상용 SW·오픈소스·내장 라이브러리 등 모든 구성요소와 알려진 취약점·대응 계획 제시

2023년 9월 발표되고 2025년 6월 업데이트된 FDA의「Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions」최종 가이드라인은 의료기기 설계·개발 단계에서 사이버보안을 내재화하고 SBOM 제출을 의료기기 품질관리 시스템(QMS)의 고려사항에 포함하도록 구체적 요구사항을 제시했다.


Contains Nonbinding Recommendations

Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions

Guidance for Industry and Food and Drug Administration Staff

Document issued on June 27, 2025.

A draft select update to this document was issued on March 13, 2024.

This document supersedes "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions," issued September 27, 2023.

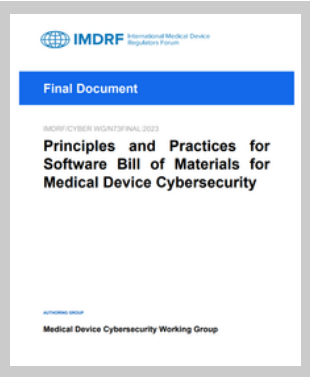
For questions about this document regarding CDRH-regulated devices, contact CyberMed@fda.hhs.gov. For questions about this document regarding CBER-regulated devices, contact the Office of Communication, Outreach, and Development (OCOD) at 1-800-835-4709 or 240-402-8010, or by email at industry.biologics@fda.hhs.gov.

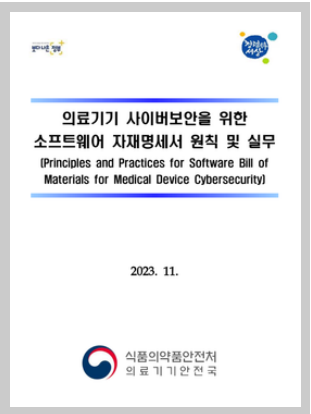
U.S. FOOD & DRUG ADMINISTRATION

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Center for Biologics Evaluation and Research

FDA「Cybersecurity in Medical Devices」가이던스
2023년 최초 제정, 2025년 개정판 발간
의료기기의 안전 확보를 위하여
설계·개발 단계에서의 사이버보안 내재화 및
SBOM 제출 의무를 규정
(출처: https://www.fda.gov/regulatory-information)

케빈 푸 교수가 미국 FDA 사례를 설명하고 있다.





IMDRF N73 문서 (2023)
전 세계 규제기관이 합의한 의료기기 사이버보안용 SBOM 원칙 및 활용 지침 최초 국제 기준 및 식약처 번역본
(출처: https://www.imdrf.org/documents/principles-and-practices-software-bill-materials-medical-device-cybersecurity)

FDA는 의료기기가 인터넷에 직접 연결되지 않더라도 Wi-Fi, 블루투스, USB 등 다양한 통신 수단을 통해 '인터넷에 연결할 수 있는 능력(ability to connect)'이 있으면 이를 사이버 디바이스로 정의해 규제 범위를 확장하였다.

미국 의료기기 사이버보안 거버넌스는 FDA뿐 아니라 NIST, CISA(사이버보안·인프라보안국), 보건복지부(HHS) 등 여러 기관이 긴밀히 협력해 통합적이고 지속 가능한 보안 정책과 기술 발전을 추진하고 있다.

HHS 산하 보건부문협력위원회(HSCC)는 산업계, 정부, 학계가 참여하는 민관 협력체계를 구축하여 Joint Security Plan(JSP) 2.0(2024) 등 의료기기 소프트웨어 전주기 보안 실무지침과 CVD(취약점 공개) 툴킷을 보급한다. 이러한 생태계는 미국 의료기기 사이버보안이 단순히 정부 규제 강화에 그치지 않고, 산업과 학계가 함께 개선을 이끄는 협력 중심 체계로 발전했음을 보여준다.

국제적 정합성 확보를 위한 움직임도 활발하다. 국제 의료기기 규제당국자 포럼(IMDRF)은 2023년 「Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity (N73)」 문서를 통해 SBOM 작성·활용 지침을 국제 공통 기준으로 제시했다. 본 문서는 식약처가 "의료기기 사이버보안을 위한 소프트웨어 자재 명세서 원칙 및 실무(N73)"라는 제목으로 번역본을 공개하기도 했다.

유럽연합(EU)은 MDR·IVDR 하위 사이버보안 지침(MDCG 2019-16 Rev.1)을 통해 취약점 관리와 보안 업데이트를 요구하고 있으며, 사이버복원력법(CRA)은 2024년 12월 발효돼 SBOM 제출 등 2027년 12월부터 주요 의무가 적용될 예정이다.

일본 의약품의료기기종합기구(PMDA)와 호주 의약품의료기기청(TGA) 또한 SBOM 기반 구성요소 관리·취약점 대응 가이드를 마련해 규제 정합성을 높이고 있다.

이처럼 의료기기 사이버보안은 국가별 편차를 넘어 국제 정합성 확보가 핵심 과제로 부상하고 있으며, 우리나라도 SBOM 기반 구성요소 관리, 취약점 대응, 민관 협력 체계의 제도화를 조기에 추진할 필요가 있다.

2.2. 국내: 「디지털의료제품법」 제정 및 사이버보안 강화

2025년 1월 24일 시행된 「디지털의료제품법」은 한국 의료기기 규제를 하드웨어 중심에서 소프트웨어와 데이터 기반 디지털 의료기기로 확대하였다. 인공지능(AI), 독립형 소프트웨어 의료기기(SaMD), 지능형 로봇, 가상·증강현실(VR·AR) 등 신기술이 적용된 제품은 '디지털 의료기기' 분류 체계의 적용을 받으며, 제품 특성·위해도·코드 산정에 따라 전환 심사(평가)와 재분류가 요구될 수 있다. 이 법은 설계·개발부터 허가, 제조·품질관리, 임상, 사후관리까지 전 주기에서 안전과 보안을 설계에 내재화하도록 요구한다.

디지털 의료제품은 ▲AI 영상진단, 로봇 수술, AR/VR 치료기기 등 진단·치료 기능 디지털 의료기기, ▲의약품에 디지털 기능을 결합한 디지털 융합 의약품, ▲헬스케어·웰니스 소프트웨어를 포함하는 디지털 의료 건강지원 기기로 구분된다. 이는 단순 정의 변경을 넘어 허가 전략, 품질관리, 보안 요구가 함께 달라질 수 있음을 의미한다.

AI가 적용된 제품은 변경관리계획(CMP) 제출이 의무다. CMP는 허가 단계에서 재학습·보안 패치·모델 교체 등의 변경 범위, 증빙, 시험·검증·배포·롤백 절차를 사전 합의해 두는 문서로, 합의 범위 내에서는 변경 처리의 리드타임을 줄여 신속한 업데이트가 가능하게 한다. 반대로 CMP의 범위가 협소하거나 구체성이 부족하면, 취약점 대응·성능 개선 시 별도 심사 부담이 커질 수 있어 개발 초기부터 업데이트 시나리오와 보안 패치 계획을 충분히 설계해 두어야 한다.

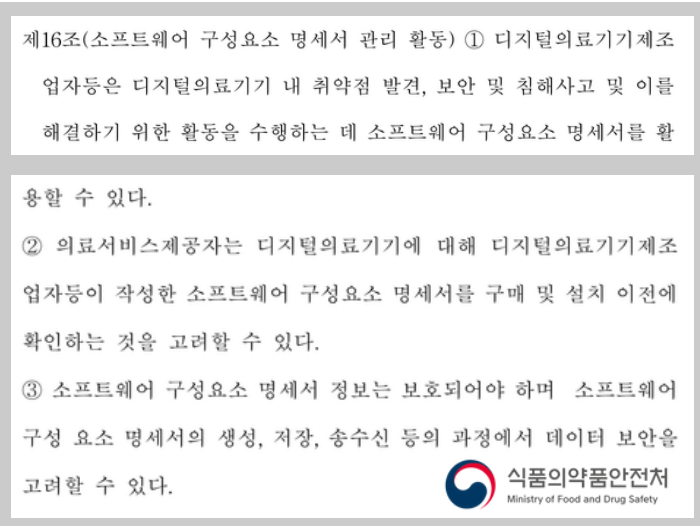
품질관리(GMP)·임상에서도 보안의 비중이 커졌다. 제조·품질관리에서는 전자적 침해 대응 절차, 위협 모델링, 취약점 관리, 데이터·암호화 방안, AI 학습 데이터 관리 등 보안 문서가 설계·품질 문서와 연계되어 준비되는 흐름이 강화되고 있다. 임상은 데이터 기반 비임상시험(시뮬레이션·의료 빅데이터) 활용 여지가 확대되면서, 실사용 데이터 무결성·접근통제·감사로그 등 보안 요소를 임상 설계와 시험계획서에 선반영하는 접근이 요구된다.

사이버보안은 2025년 4월 식약처 고시 「디지털의료기기 전자적 침해행위 보안지침」(제2025-30호)으로 한층 세분화되었다. 이 지침은 해킹·랜섬웨어·데이터 변조뿐 아니라 AI 모델 추출·중독·회피 등 AI 특유의 위협까지 고려한 다층 방어를 권고한다. 물리적 보안(시설 출입 통제, 사용자·관리자 인증, 반입·반출 관리)과 기술적 보안(무결성·암호화키 관리, 취약점 대응 절차, 실시간 모니터링)을 포괄하며, 소프트웨어 구성요소와 취약점 관리를 위한 SBOM 활용을 명시적으로 다룬다. 본 지침은 법적 강제 규정은 아니지만, 허가·심사에서 기술적 보안 수준을 입증하는 근거로 활용될 가능성이 높다. FDA·EU의 의무화 기조를 고려하면 해외 시장을 목표로 하는 기업에는 SBOM이 사실상 필수 준비 항목이다.

현장 적용을 돕기 위해 식약처는 디지털의료제품 규제지원센터를 운영하며 인허가 상담, 품질·임상 컨설팅을 제공한다. 사이버보안 분야는 한국정보통신기술협회(TTA) 등이 참여해 보안 설계 검토, SBOM 구축, 보안 시험 계획 수립 등 실무 지원을 제공한다. 스타트업·중소기업은 초기 설계 단계부터 이 지원을 활용하면 시행착오를 줄이고 준비 기간을 단축할 수 있다.

실무 관점에서의 우선순위는 분명하다. 첫째, 자사 제품이 디지털 의료기기 분류와 새 등급 체계의 적용 대상인지 사전 판별한다(제품 정의, 위해도, 연결성·데이터 처리 유무 중심). 둘째, 허가 단계에서 CMP에 재학습·보안 패치의 범위/증빙/검증·배포/롤백을 구체화해 규제·기술 전략을 동기화한다. 셋째, 설계 단계에서 위협 모델링→보안 아키텍처→SBOM 운영→취약점 대응 절차→로그/추적성을 품질 문서(DHF/DMR 등)와 연동해 일괄 문서화한다. 넷째, 비임상/임상 계획에 보안 시험(침해 시나리오, 안전성 검증)과 데이터 무결성 검증을 포함한다. 다섯째, 국내 법 의무화 전이라도 SBOM 운영·취약점 공개(CVD) 프로세스를 FDA 기준에 맞춰 설계해 해외 고객·심사 대응 시간을 단축한다. 아울러 의료 데이터의 민감성을 고려해 개인정보보호법 연계 통제, 사고 대응 훈련, 인력·조직 역량 강화도 병행해야 한다.

최근의 국내법은 “보안을 사후 점검이 아닌 설계 기본값으로 만들라”는 방향을 명확히 했다. 정부는 CMP·SBOM 표준 템플릿과 샘플 문서, 연결성·데이터 흐름 다이어그램 표준, 보안 시험 참조 시나리오를 공개해 중소기업의 초기 비용을 낮추고, 산학연 네트워크를 통한 분기별 클리닉(문서 리뷰·사전검토) 등으로 실행력을 높일 필요가 있다. 산업계는 제품 설계 전부터 SBOM 운영 체계 등 보안 내재화를 우선 과제로 삼아 글로벌 규제와의 정합성을 선제 확보하는 것이 비용 대비 효과가 높다.



제16조(소프트웨어 구성요소 명세서 관리 활동) ① 디지털의료기기제조업자등은 디지털의료기기 내 취약점 발견, 보안 및 침해사고 및 이를 해결하기 위한 활동을 수행하는 데 소프트웨어 구성요소 명세서를 활용할 수 있다.

② 의료서비스제공자는 디지털의료기기에 대해 디지털의료기기제조업자등이 작성한 소프트웨어 구성요소 명세서를 구매 및 설치 이전에 확인하는 것을 고려할 수 있다.

③ 소프트웨어 구성요소 명세서 정보는 보호되어야 하며 소프트웨어 구성 요소 명세서의 생성, 저장, 송수신 등의 과정에서 데이터 보안을 고려할 수 있다.

식품의약품안전처 Ministry of Food and Drug Safety

「디지털의료기기 전자적 침해행위 보안지침」
(식약처 고시 제2025-30호, 2025.4.29.)
(출처: https://www.mfds.go.kr/brd/m_211/view.do?seq=14894)

IoTcube Conference 2025에서 식품의약품안전처 디지털의료제품TF 손미정 팀장이 디지털의료제품법에 대해 설명하고 있다.

3. 대응 기술의 부상: SBOM과 VEX

3.1. 초복잡 사이버-물리 시스템으로 진화한 의료기기

현대 의료기기는 센서·펌프·로봇 등 물리적 구성요소와 이를 제어하는 펌웨어·알고리즘·AI 모듈이 결합된 초복잡 사이버-물리 시스템(Cyber-Physical System)이다. 환자 생체 신호를 실시간 처리해야 하므로 보안 결함은 곧 환자 안전 문제로 직결된다.

Synopsys의 OSSRA 보고서에 따르면, 헬스케어·생명과학 분야 코드베이스의 93%가 오픈소스를 포함(2022)하고, 80%에서 고위험 취약점이 발견(2025)되었다. MongoDB·TensorFlow·Linux 등 핵심 오픈소스조차 수십 단계의 의존성을 내장해, 한 곳의 취약점이 전체 제품으로 전파될 가능성이 크다.

기존의 방화벽·암호화·접근통제 등 경계 중심 보안만으로는 이러한 위협에 대응하기 어렵다. 수많은 외부 구성요소가 얽힌 의료기기는 사실상 블랙박스에 가까워, 어디에 어떤 소프트웨어가 들어 있는지조차 파악하기 힘든 '가시성(visibility) 부족)'이 가장 큰 위협으로 지적된다.

이런 배경에서 소프트웨어 공급망 보안(Software Supply Chain Security) 개념이 의료기기 보안에도 본격적으로 부상하고 있다. 소프트웨어 공급망 보안은 제품에 포함된 모든 소프트웨어 구성요소출처·버전·취약점 상태를 투명하게 파악·관리해, 취약점 발생 시 어떤 제품이 영향받는지 신속히 식별·대응하는 체계를 말한다.

이 공급망 보안을 현실화하는 핵심 기술이 바로 SBOM과 VEX다.

- **SBOM (Software Bill of Materials, 소프트웨어 자재명세서)**
제품에 포함된 모든 소프트웨어 구성요소(패키지·버전·공급자 등)를 목록화한 문서로, 각 구성요소 출처·의존관계를 가시화해 취약점 추적·패치·위험평가를 가능케 함 (SPDX, CycloneDX 형식 활용)

- **VEX (Vulnerability Exploitability eXchange, 취약점 상태 기술 표준 문서)**
SBOM으로 확인된 취약점이 실제 제품에서 악용 가능한지 여부(affected/not affected/fixed 등)를 기계판독 가능한 형식으로 제공하는 문서로, 수백 건의 알려진 취약점 중 실제 대응 필요한 항목만 선별하도록 지원

즉, SBOM은 '무엇이 들어있는지', VEX는 '무엇이 실제로 위험한지'를 알려주는 도구이며, 두 기술이 함께 활용될 때 의료기기 공급망 보안과 규제 대응의 실효성을 획기적으로 높일 수 있다.

3.2. 의료기기 보안 전략의 3단계

이희조 교수는 고려대학교 컴퓨터학과 교수이자 소프트웨어보안연구소(CSSA) 연구소장이다. 2015년부터 보안 취약점 자동분석 오픈 플랫폼 IoTcube를 연구했으며, 기업용 보안 솔루션 래브라도랩스 공동 CEO로도 활동 중이다.

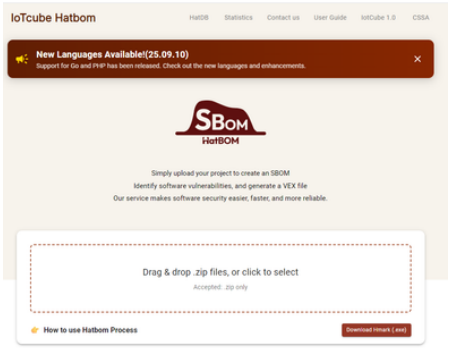
고려대학교 이희조 교수는 복잡한 SW로 구성된 현대 의료기기 특성상 개발 전 과정에 보안 내재화 → 구성요소 가시화 → 운영 단계 검증의 3단계 전략을 제시했다.

이 전략을 누구나 활용할 수 있도록, 고려대 소프트웨어보안연구소(CSSA)에서는 국제공동연구팀이 최우수 학회에서 발표한 취약점 분석·SBOM 자동생성·VEX 기반 기술을 도구화하여 IoTcube.net 오픈 플랫폼으로 공개하고 있다.

1) 보안 내재화(Secure SDLC)
- 개발 초기부터 보안 검증 포함해 설계 단계에서 취약점 예방
- IoTcube 플랫폼의 Vuddy(대규모 취약 코드 패턴 탐지, IEEE S&P '17), Cneps(오픈소스 의존성 분석, ICSE '24) 기술로 코드 단계부터 취약점 사전 탐지

2) 구성요소 가시화(SBOM)
- 제품 포함된 SW 구성요소(공급자 등)를 투명하게 목록화
- 소스코드·바이너리를 분석해 SBOM 및 VEX를 자동 생성하는 IoTcube 2.0(Hatbom) 도구 활용 제안
- SBOM 기반 오픈소스 라이선스·취약점·EOL 상태 사전 점검

3) 운영 단계 취약점 검증(VEX)
- SBOM으로 파악된 취약점 중 악용 가능한 항목 위주 관리
- 분석 결과를 VEX 문서 자동 생성·배포하는 파이프라인 연구 진행 중



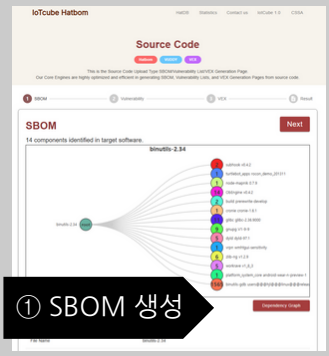
SBOM 생성 및 관리를 위한 IoTcube 2.0 (Hatbom) 메인 페이지 (https://iotcube.net)

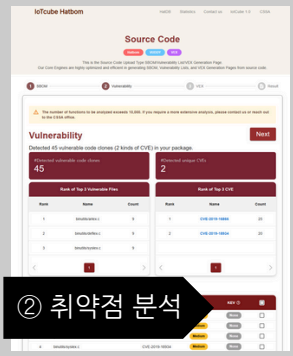
3단계 전략을 꾸준히 적용하면 의료기기 기업은 소프트웨어 공급망 전반 투명성·신뢰성·안전성을 확보하고, 강화되는 국제 규제와 시장 요구에 대응할 기술 경쟁력을 갖출 수 있다.

현재 CSSA는 미국 Georgia Tech·Northeastern University, 스위스 ETH Zurich, 한국 KAIST·KISIA(정보보호산업협회) 등과 SBOM 및 VEX 기반 보안 기술을 공동 연구하며, 산업계 실사용에 기여하고 있다.

보안취약점 자동분석 플랫폼 IoTcube 2.0: Hatbom

고려대 소프트웨어보안연구소(CSSA)는 10년간의 국제 공동연구 성과를 바탕으로 차세대 오픈 플랫폼 'IoTcube 2.0(Hatbom)'을 런칭했다. Hatbom은 소스코드 입력만으로 SBOM 생성 → 취약점 분석 → VEX 문서화 원스톱 프로세스를 지원하는 보안취약점 자동 분석 플랫폼으로, 의료기기를 비롯한 소프트웨어 기반 제품 보안·규제 대응 준비를 도울 수 있다.





아이오티큐브 2.0
체험하기
https://iotcube.net

Hatbom 3단계 원스톱 프로세스

① SBOM 생성

- 사용자는 소스코드 또는 해시 암호화된 파일 업로드 (차후 바이너리·컨테이너·URL 등 지원 예정)
- 복잡한 설정 없이 플랫폼이 자동으로 소프트웨어 자재명세서(SBOM)를 생성
- 제품에 포함된 구성요소의 패키지·버전·공급자·의존관계까지 투명하게 가시화

② 취약점 분석

- 단순 나열이 아닌, 실제 악용 가능성이 높은 취약점에 집중
- 전체 중 약 5%의 고위험 취약점 코드 존재 여부와 도달 가능성(reachability) 평가
- 기업이 위험도 기반 우선순위 설정 및 대응 전략 수립 가능

③ VEX 문서화

- 분석 결과를 VEX(Vulnerability Exploitability eXchange) 형식으로 변환
- 각 취약점의 실제 위험 여부(affected / not affected)와 데이터 흐름·보안 상태 변화를 시각적 대시보드로 제공
- 기업이 보안 리스크를 직관적으로 파악하고 대응 전략 수립 가능

※ Hatbom은 학계 연구결과 기반 무료 플랫폼으로, 기업용 상용화는 (주)래브라도랩스(Labrador Labs) 문의 요망 / https://labradorlabs.ai

3.3. SBOM·VEX 기술 신뢰성과 임상의 연결

SBOM과 VEX가 공급망 보안의 실질적 도구가 되려면 기술적 정확성과 현장(임상) 타당성이 함께 확보돼야 한다. 기술 연구와 현장 적용 사이의 간극을 메우기 위한 두 가지 접근도 소개됐다.

차상길 교수는 KAIST 정보보호대학원 교수이자 사이버보안연구센터(CSRC) 센터장이다. 보안·프로그램 분석 전문가로 IEEE S&P Test-of-Time Award 한국인 최초 수상자이기도 하다.

KAIST **차상길** 교수는, 빌드 단계에서 컴파일러가 생성한 어셈블리 코드를 기계어로 변환하는 어셈블러 오류가 전체 보안 분석을 흔들 수 있음을 지적했다. 어셈블러는 어셈블리 코드를 CPU가 이해하는 기계어로 바꾸는 핵심 도구이기 때문에, 이 단계에서 변환 오류가 발생하면 소스코드 수준의 의미와 최종 바이너리의 실제 동작이 달라져 취약점 판단과 대응이 잘못될 수 있다.

이 문제를 해결하기 위해, 연구팀은 여러 어셈블러를 자동으로 비교하고 오류를 찾아내는 ASFuzzer를 개발해 대규모의 버그를 발견했다. 이처럼 빌드 도구의 신뢰성을 높이는 것이 소스코드와 공급망 보안과 취약점 검증의 출발점임을 강조했다.

제프 툴리(Jeff Tully)는 UC San Diego(UCSD) 마취과 임상 부교수이자 Center for Healthcare Cybersecurity 공동 책임자다. 의대 진학 전 살모넬라 박테리아 유전 암호를 해킹해 항암 도구를 개발했으며, 원격 진료·이식형 의료기기·바이오해킹 등 차세대 의료 환경의 보안 연구를 이어가고 있다.

UC 샌디에이고 **제프 툴리(Jeff Tully)** 교수는 마취과 의사이자 보안 연구자로서 “보안은 기술만의 문제가 아니라 환자 안전 문제”임을 강조했다. 그는 실제 병원 환경을 재현한 임상 시뮬레이션을 설계해, 의료기기가 해킹되거나 오작동할 때 의료진이 어떻게 반응하는지 실험했다.

예를 들어, 당뇨 환자가 교통사고 후 실려왔지만 혈당이 급격히 떨어진 상황을 만들었을 때 의료진은 장비 오작동이나 사이버 공격을 전혀 의심하지 않고 일반적 저혈당 치료에만 집중했다. 이런 장면을 통해 기술적 취약점 연구를 임상적 스토리로 바꿔야 현장에서 의미가 살아난다는 점을 보여주었다. 세션에서는 병원 보안 인력 부족, 책임 주체 분산 등 현실적 제약도 함께 논의됐다.

결국 SBOM·VEX 같은 공급망 보안 도구가 실질적 환자 보호 수단으로 발전하려면 분석 단계의 기술적 신뢰성과 현장에서의 임상적 검증이 같은 언어로 연결돼야 한다. 기술자·임상의·보안 담당자의 협업이 선순환을 만들 때만 SBOM·VEX는 단순 규제 대응을 넘어 의료기기 안전과 산업 경쟁력까지 끌어올릴 수 있다.

4. 현장 SBOM 적용 사례와 교훈

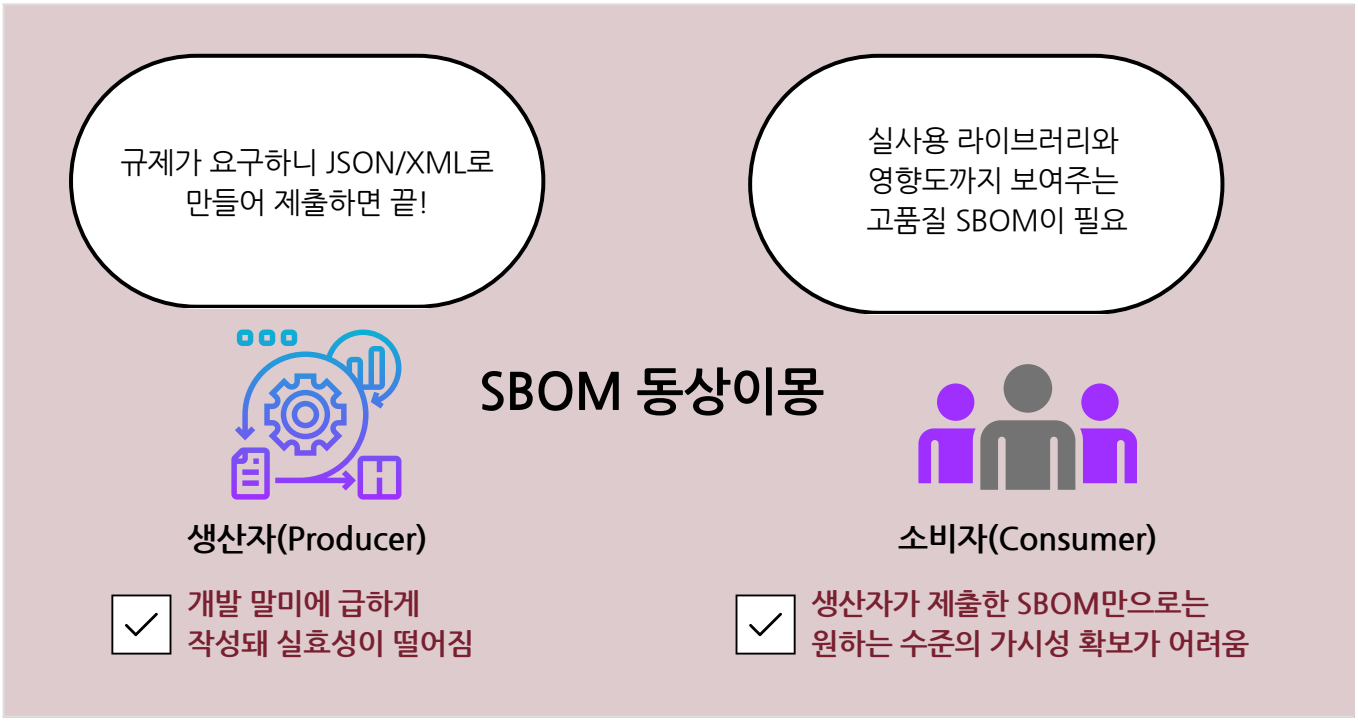
최근 소프트웨어 공급망 공격이 급증하면서 SBOM(Software Bill of Materials)이 중요한 보안 수단으로 떠오르고 있다.

2020년 솔라윈즈(SolarWinds) 취약점 해킹, 미 동부 송유관을 마비시킨 2021년 콜로니얼 파이프라인(Colonial Pipeline) 공격 등 대형 사고를 겪으며 미국, 유럽 등은 SBOM 제출을 의무화하는 규제를 도입했다.

미국 바이든 행정부는 2021년 행정명령을 통해 공공기관 납품 제품의 SBOM 제출을 의무화했고, NTIA·NIST·CISA가 세부 지침을 마련했다. 유럽 역시 ENISA와 CRA(Cyber Resilience Act)를 중심으로 규제를 강화했으며, 한국도 2023년 공급망 보안 가이드라인을 발표했다. 의료·금융·공공 등 일부 부처는 빠르게 제도를 준비하고 시행을 시작했다.

오늘날 SBOM은 특정 산업을 넘어 자동차·의료기기·통신·소프트웨어 전반에서 공통 보안 요건으로 자리 잡고 있다.

그러나 현장에서 SBOM 도입을 달가워하는 목소리만 존재하는 것은 아니다. 삼성전자 네트워크 사업부 **김유승 상무**는 IoTcube Conference 2025에서 실제 SBOM을 적용하며 겪은 시행착오와 교훈을 공유했다.



기업 내 SBOM 적용 시 현장 난관

구분	사례
내부 조직의 심리적 거부감	“왜 해야 합니까? 너무 바빠요.” → SBOM 필요성 이해 차이로 인한 갈등
수집 방식 혼란	“소스 코드, 바이너리, 패키지 중 무엇을 수집해야 하나요?” → 소스코드, 바이너리, 패키지 모두 필요. 특정 관점만으로는 불충분
도구의 한계	대규모 프로젝트(수십~수백 GB) 스캔에 최대 5일 소요. 현재는 자동화로 소요 시간을 단축했으나, 성능·정확도·편의성 균형은 여전히 과제
정확도 문제	실제 사용하지 않는 라이브러리 포함 → 불필요한 CVE 경고 발생 / 누락 라이브러리 뒤늦게 발견

“SBOM은 느리고 복잡해 보이지만 제대로 내재화하면 개발·운영을 더 빠르게 만드는 무기”

김유승 상무는 이러한 어려움에도 불구하고, SBOM 내재화는 규제 준수를 넘어 기업의 핵심 경쟁력이 된다고 강조했다.

김유승 삼성전자 네트워크사업부 상무는 통신 시스템, 의료기기, 자동차 보안 등 미션 크리티컬 시스템의 위협 분석과 대응책 개발에 주력해 왔다.

SBOM의 사업적 가치는 다음과 같다

- **위기 대응 속도:**
  Log4j와 같은 중요 이슈를 수개월→하루 단위 파악·조치 단축 가능
- **공급망 신뢰:** 고객·협력사와 가시성·책임 분담을 계약으로 제도화
- **제품 경쟁력:** “규제서류”가 아니라 신뢰·품질을 증명하는 영업자산

김 상무는 “SBOM은 단순한 문서 작업으로 개발 속도를 늦추는 족쇄가 아니라, 취약점을 신속히 대응하는 레이더이며 신뢰를 얻는 경쟁력”이라고 덧붙였다.

SBOM을 “살아있는 자산“으로 사용하기 위한 5가지 운영 원칙

Insights from IoTcube Conference 2025

1. CI/CD 내재화 (Design → Build → Release → Operate)

- 코드 개발과 배포 자동화 파이프라인(CI/CD)에 SBOM 생성·검증을 통합
- PR 단계에서는 경량 스캔, 릴리즈 전에는 정밀 스캔, 배포 후에는 자산 인벤토리 자동 업데이트
- 버전·빌드번호·커밋 해시와 연계해 SBOM의 추적 가능성(traceability) 확보

2. 지속 동기화 (Continuous Sync)

- SBOM은 한 번 만들고 끝나는 문서가 아니라 지속 업데이트 자산
- 신규 취약점(CVE) 발생 시 자동 감지 및 심각도 기반 라우팅 → 담당자·서비스 팀 알림
- KEV(실제 악용된 취약점 목록)를 우선 모니터링, 중요 서비스는 시간 단위·일반 서비스는 일 단위 동기화

3. VEX로 ‘의미’ 부여

- 단순 “존재 여부”가 아니라 “우리 제품에 실제 영향이 있는가”까지 표준 포맷(VEX)으로 제공
- 불필요한 경보를 줄이고, 계약·감사·분쟁 대응 시 근거 자료로 재활용 가능

4. 거버넌스와 문화

- 보안팀 전담이 아닌 Dev·QA·Ops·ProdSec 공동 책임 구조(공동 OKR 설정)
- 배포 여부(Stop/Go)를 정책 코드화(policy-as-code)하여 자동 의사결정 체계 마련
- 현장의 “왜?”라는 반발은 서비스 수준 목표(SLO)로 설명·설득 (예: Critical ≥7 → 7일 내 조치)
- 조직 여건에 따라 단계적 적용을 권장, 핵심 릴리즈 게이트부터 시작

5. 공급망 계약화 (Up/Down-stream)

- SBOM/VEX 제공 주기, 포맷(SPDX·CycloneDX), 감사 권한을 계약에 명시
- CVE 심각도별 대응 기한을 계약에 포함 (예: Critical → 24시간 내 영향평가, 7일 내 완화)
- 계약을 통해 책임과 기대치를 상호 대칭적으로 설정, 분쟁·리스크 최소화

5. 시사점

고려대학교 소프트웨어보안연구소(CSSA)는 노스이스턴대 Archimedes Center for Healthcare and Medical Device Cybersecurity와 함께 IoTcube Conference 2025를 공동 주최하며, 의료기기 사이버 보안과 글로벌 공급망 보안을 논의하는 국제 협력의 장을 마련했다. 이번 컨퍼런스는 SBOM·VEX의 실제 도입 경험과 국제 규제 동향을 공유하고, 산업계·학계·규제기관이 직면한 기술적·정책적 과제를 종합적으로 점검한 자리였다.

이번 논의는 의료기기 보안이 더 이상 기술적 선택이 아니라 환자 안전과 산업 신뢰를 지키는 필수 조건임을 분명히 했다. 연사들은 초복잡화된 소프트웨어 구조 속에서 기존 방어만으로는 한계가 뚜렷하며, 정확한 구성요소 파악(SBOM)과 실제 악용 가능성 판별(VEX)이 대응력의 핵심임을 강조했다. 동시에 개발 단계 보안 내재화, 자동화 기반의 SBOM 생성과 갱신, 임상 환경과의 소통 강화 등 기술적·조직적 개선 시도가 공유되며, SBOM과 VEX를 '규제 대응 문서'가 아닌 살아 있는 보안 자산으로 운영해야 한다는 공감대가 확산됐다.

참석자 만족도 조사 또한 방향성을 뒷받침했다. 프로그램의 전문성과 시의성에 대한 높은 평가와 함께, 명확한 정책 가이드라인과 기업 지원 수단, 국제 규제 사례 및 실행 전략 공유에 대한 요구가 도출되었다. 이는 업계의 실질적 필요와 정책적 후속 조치 간 간극을 메울 구체적 실행 프레임워크가 필요함을 시사한다.

이 논의를 토대로 도출된 시사점은 다음과 같다.

1) (기업) SBOM·VEX 활용 역량 내재화와 산업 구조적 정착

- 기업에게 SBOM은 더 이상 "보유 여부"가 아니라 위험 선별과 대응 역량의 문제다. 수백 건의 취약점 중 실제 악용 가능성이 높은 약 5%만을 신속히 분리하고 대응하는 것이 핵심이다. 이를 위해 VEX 기반 영향도 분석과 CI/CD 파이프라인 내 보안 자동화가 필수이며, 정부와 산업 단체는 이를 평가·인증 및 조달 조건과 연계해 기업이 보안 내재화를 산업 표준으로 받아들이도록 유도할 필요가 있다.

2) (정부) SBOM 기반 공급망 보안 제도화 및 중소·중견기업 지원 강화

- 정부는 공급망 보안 제도화를 공공부문부터 단계적으로 추진해 민간 확산 기반을 마련할 필요가 있다. 특히 정부기관 및 산하기관이 도입하는 시스템에 SBOM 제출과 보안 관리 체계를 먼저 적용하고, 이를 효율적으로 운영·감독할 수 있는 표준 절차를 준비해야 한다. 아울러 인력과 자원이 부족한 중소·중견기업을 위해 SBOM 자동화 도구 바우처, 모범 사례와 참조 아키텍처, 오픈소스·SaaS 활용 지원, 보안 역량 교육 등 저비용·고효율 진입 모델을 제공해 초기 부담을 덜어줄 필요가 있다. 이러한 노력은 개별 기업 보호를 넘어 공급망 전체 취약 지점을 완화하고 국가 방어력을 높이는 투자다.

3) (인허가 기관) 예측 가능한 평가체계와 한국형 가이드라인 마련

- “FDA 모델을 참고하는 것은 좋지만, 한국형 모델이 필요하다”는 현장 요구가 반복됐다. 규제기관은 업계·학계와 정례적으로 소통하며 한국형 SBOM·VEX 가이드라인을 수립하고, CI/CD 내재화·지속 동기화·VEX 활용 등 실무에서 검증된 원칙을 허가·인증 단계에 반영해야 한다. 공개된 보안성 평가 모델과 인증 체크리스트를 마련해 기업이 준비 방향과 비용을 예측 가능하게 하고 혁신적 제품의 시장 진입을 촉진해야 한다.

4) (학계) 연구 성과의 실질적 전환과 국제 표준화 리더십

- 학계는 기술 성과를 산업이 활용할 수 있는 도구와 검증 체계로 연계해야 하며, 정부는 이를 R&D 단계부터 표준화와 정책과 연계하도록 지원해야 한다. 오픈소스화, 상호운용성 검증, 국제 표준화 참여를 통해 국내 기술을 글로벌 규제와 시장의 공통 언어로 만들고, 한국이 기술-정책-산업을 잇는 보안 허브로 자리매김하도록 뒷받침해야 한다.

5) (글로벌) 연계·공유 생태계와 국가 차원의 협력 허브 구축

- 공급망 보안은 단일 조직만으로 완성되지 않는다. 기업·정부·규제기관·학계가 취약점 데이터와 대응 지침을 투명하게 공유하고, SBOM·VEX 제공 주기와 대응 목표를 표준 계약과 법적 가이드라인으로 명문화해야 한다. 정부는 이를 뒷받침할 국가 취약점 관리·정보 공유 플랫폼을 마련해 공공-민간이 동일한 기준과 데이터를 활용하도록 지원해야 한다. 동시에 국제 협력이 필수적이다. FDA, NTIA, CISA 등 글로벌 규제·정보 공유 체계와 긴밀히 연계하고 국제 표준화 활동을 주도함으로써 한국이 의료기기와 더 넓은 산업 전반에서 글로벌 보안 신뢰 허브로 자리잡도록 해야 한다.

기술 내재화와 정부의 전략적 지원, 규제기관의 예측 가능성, 학계의 표준화 주도, 그리고 산업 전반의 연계 생태계가 국제 협력과 국가 차원의 정책적 거버넌스와 맞물릴 때 한국은 공급망 보안의 취약 고리를 최소화하고, 글로벌 의료기기 시장에서 신뢰와 경쟁력을 동시에 선도할 수 있을 것이다.

고려대 소프트웨어보안연구소(CSSA)는 8월 26일 서울 JW 메리어트 동대문 스퀘어 서울에서 ‘제9회 IoTcube 컨퍼런스’를 개최했다.

부록: 패널토의 Q&A

Q1. 의료기기 사이버보안 심사 과정에서 승인 실패 사례와 교훈은 무엇인가요?

Kevin Fu 교수(노스이스턴대, 前 미국 식품의약국(FDA) 의료기기 보안 책임자)는 “수십억 달러 규모 제품도 보안 문제로 승인이 거절되는 경우가 있었다”며, 주요 실패 원인으로 위협 모델링 부재와 ‘우리 제품에는 보안 문제가 전혀 없다’는 현실적이지 않은 주장을 꼽았다. 그는 규제기관이 원하는 것은 “문제가 없는 제품”이 아니라 “문제가 발생했을 때 어떻게 관리하는지”라고 강조했다.

손미정 팀장(식품의약품안전처)은 “심사 과정에서 가장 중요한 것은 문서 입증”이라며, 설계부터 출시까지 보안을 지속 관리하고, 업데이트나 변경이 있을 때 중요 변경 여부를 기업 스스로 입증할 수 있어야 한다고 설명했다. 또한 개발 단계와 최종 제출 단계가 달라질 수 있으므로 초기부터 규제 요구사항을 파악하고 규제지원센터와 가이드라인을 적극 활용할 것을 권고했다.

김유승 상무(삼성전자)는 “새로운 프로젝트 초기에는 ‘누가 보안 승인 권한을 갖는지, 책임이 어느 부서인지’가 불분명해 혼란이 있었다”고 경험을 공유하며, 부서 간 역할을 조율하고 외부 승인 기관과 협력해 거버넌스를 정립하는 과정이 기업 보안 역량 강화의 핵심이라고 말했다.

이희조 교수(고려대)는 “국내 기업들은 디지털의료제품법 등 익숙하지 않은 신규 인증 절차에 어려움을 겪고 있다”며 두 사례를 들었다. 첫째, 지원 종료(EOL) 소프트웨어가 포함된 상태로 인증을 시도해 승인을 받지 못한 사례, 둘째, 한 제품에서 수천 개의 취약점(CVE)이 발견됐지만 적절한 대응 방안을 제시하지 못해 인증이 지연된 사례였다. 그는 “인증 통과만을 목표로 하기보다 개발 초기부터 보안을 내재화하고 SBOM·VEX를 활용해야 한다”고 강조했다.

IoTcube Conference 2025 패널토의 세션

< 디지털 의료제품 규제지원센터 >

- **(지정근거)** 「디지털의료제품법」제45조
- **(지원분야)** ❶디지털의료제품의 개발, 임상시험 등 안전성·유효성 평가를 위한 규제지원, ❷디지털의료제품 전자적 침해행위의 예방 및 확산 방지를 위한 규제지원
- **(지정기관)** ❶한국스마트헬스케어협회, ❷한국정보통신기술협회
- **(지정기간)** ‘25.4.29~ (3년간)
- **(지원내용)**
  - 정책지원: 규제 동향 보고서 발간, 규제해설서 배포
  - 인력양성: 교육교재 개발, 설명회·교육 실시
  - 기술지원: 제도 관련 컨설팅, 규제 관련 사례집(FAQ) 발간, 유관기관 연계

식약처, ‘디지털의료제품 규제지원센터’ 지정 보도자료 (2025.04.)

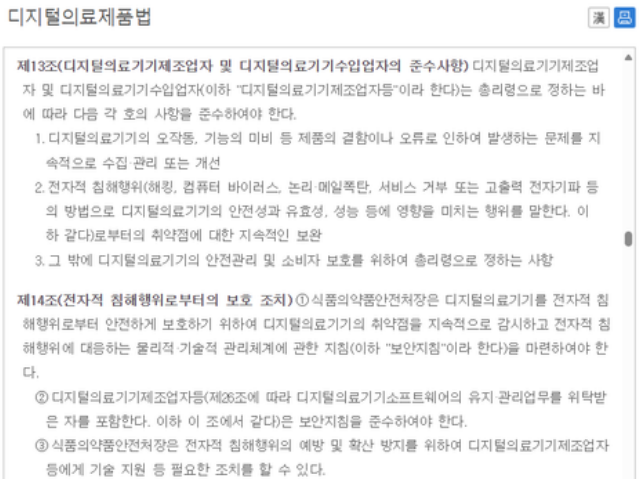
Q2. SBOM/VEX를 도입했을 때 규제 대응과 보안 관리에 어떤 도움이 되나요?

김유승 상무는 “Log4j 취약점 사태 때 우리 제품이 영향을 받는지 확인하기 위해 개발자에게 일일이 문의하고 문서를 찾아보는 혼란이 있었다”고 회상했다. 그는 “SBOM 체계가 구축되면 공개된 취약점이 제품에 미치는 영향을 즉시 파악할 수 있어 대응 속도가 훨씬 빨라진다”며, “초기 SBOM 시스템을 만들고 내부 문화를 정착시키는 데 1년 이상 걸렸지만 이후에는 보안 인식과 대응 효율이 크게 향상됐다”고 강조했다.

이희조 교수는 “SCA(소프트웨어 구성 분석) 기반의 SBOM 관리는 해외 수출 시 규제기관과 고객에게 신뢰를 제공하는 강력한 증명 수단”이라며, 개발·배포·운영 전 단계에서 SBOM을 일관되게 적용하는 것이 장기 경쟁력 확보에 중요하다고 조언했다.

Kevin Fu 교수는 “미국은 의료기기 분야 SBOM 제출을 법으로 의무화했다”라며, FDA는 단순 제출 여부가 아니라 각 항목을 미국 국가 취약점 데이터베이스(NVD)와 대조해 위험도를 평가하고, 취약점이 있더라도 ‘보상적 통제(compensating control)’를 통해 어떻게 관리·완화하는지를 요구한다고 설명했다.

손미정 팀장은 “국내는 SBOM 제출이 의무가 아니지만 미국과 같은 해외 규제 사례가 존재하기 때문에 수출을 염두에 둔다면 대응이 필요하다”고 설명했다. 유럽은 아직 SBOM 제출을 의무화하지 않았지만 MDR 이후 인공지능 기반 제품이나 전환기 제품에 대한 심사가 강화되는 추세다. 대한민국도 회원으로 참여 중인 국제 의료기기 규제당국자 포럼(IMDRF)에서도 글로벌 정합을 위한 논의가 활발하며, SBOM 활용 가이드라인도 존재한다. 국내에서는 최근 디지털의료제품법을 기반으로 전자적 침해행위 보안지침을 제정해 사이버보안 심사 자료를 준비할 수 있게 안내 중이며, 국내 의료기기 제조·판매·수입 기업이 이를 참조할 필요가 있다고 밝혔다.



디지털의료제품법

제13조(디지털의료기기제조업자 및 디지털의료기기수입업자의 준수사항) 디지털의료기기제조업자 및 디지털의료기기수입업자(이하 "디지털의료기기제조업자등"이라 한다)는 총리령으로 정하는 바에 따라 다음 각 호의 사항을 준수하여야 한다.

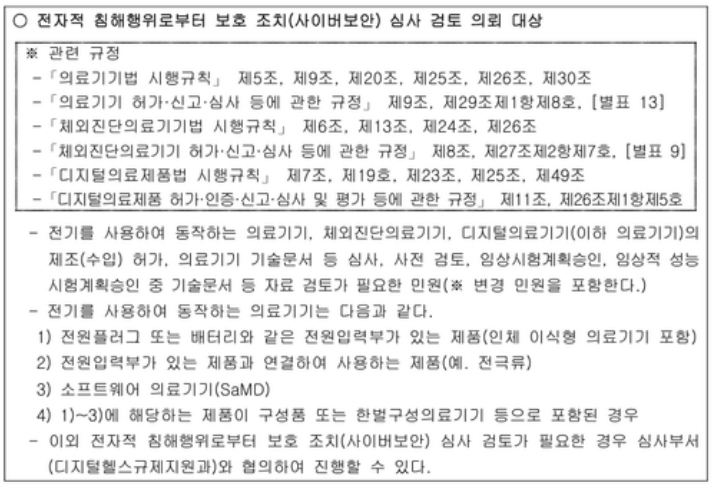
1. 디지털의료기기의 오작동, 기능의 미비 등 제품의 결함이나 오류로 인하여 발생하는 문제를 지속적으로 수집 관리 또는 개선
2. 전자적 침해행위(해킹, 컴퓨터 바이러스, 논리 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 디지털의료기기의 안전성과 유효성, 성능 등에 영향을 미치는 행위를 말한다. 이하 같다)로부터의 취약점에 대한 지속적인 보완
3. 그 밖에 디지털의료기기의 안전관리 및 소비자 보호를 위하여 총리령으로 정하는 사항

제14조(전자적 침해행위로부터의 보호 조치) ① 식품의약품안전처장은 디지털의료기기를 전자적 침해행위로부터 안전하게 보호하기 위하여 디지털의료기기의 취약점을 지속적으로 감시하고 전자적 침해행위에 대응하는 물리적 기술적 관리체계에 관한 지침(이하 "보안지침"이라 한다)을 마련하여야 한다.

② 디지털의료기기제조업자등(제26조에 따라 디지털의료기기소프트웨어의 유지 관리업무를 위탁받은 자를 포함한다. 이하 이 조에서 같다)은 보안지침을 준수하여야 한다.

③ 식품의약품안전처장은 전자적 침해행위의 예방 및 확산 방지를 위하여 디지털의료기기제조업자등에게 기술 지원 등 필요한 조치를 할 수 있다.

디지털의료제품법 제14조: 전자적 침해행위로부터의 보호 조치



○ 전자적 침해행위로부터 보호 조치(사이버보안) 심사 검토 의뢰 대상

※ 관련 규정
- 「의료기기법 시행규칙」 제5조, 제9조, 제20조, 제25조, 제26조, 제30조
- 「의료기기 허가·신고·심사 등에 관한 규정」 제9조, 제29조제1항제8호, [별표 13]
- 「체외진단의료기기법 시행규칙」 제6조, 제13조, 제24조, 제26조
- 「체외진단의료기기 허가·신고·심사 등에 관한 규정」 제8조, 제27조제2항제7호, [별표 9]
- 「디지털의료제품법 시행규칙」 제7조, 제19호, 제23조, 제25조, 제49조
- 「디지털의료제품 허가·인증·신고·심사 및 평가 등에 관한 규정」 제11조, 제26조제1항제5호

- 전기를 사용하여 동작하는 의료기기, 체외진단의료기기, 디지털의료기기(이하 의료기기)의 제조(수입) 허가, 의료기기 기술문서 등 심사, 사전 검토, 임상시험계획승인, 임상적 성능시험계획승인 중 기술문서 등 자료 검토가 필요한 민원(※ 변경 민원을 포함한다.)
- 전기를 사용하여 동작하는 의료기기는 다음과 같다.
  1) 전원플러그 또는 배터리와 같은 전원입력부가 있는 제품(인체 이식형 의료기기 포함)
  2) 전원입력부가 있는 제품과 연결하여 사용하는 제품(예. 전극류)
  3) 소프트웨어 의료기기(SaMD)
  4) 1)~3)에 해당하는 제품이 구성품 또는 한벌구성의료기기 등으로 포함된 경우
- 이외 전자적 침해행위로부터 보호 조치(사이버보안) 심사 검토가 필요한 경우 심사부서(디지털헬스규제지원과)와 협의하여 진행할 수 있다.

전자적 침해행위로부터 보호 조치(사이버보안) 심사 검토 의뢰 대상
(출처: 식약처 공무원 지침서 (1063-01-3411))

Q3. SBOM의 신뢰성과 공증은 어떻게 확보할 수 있을까요?

이희조 교수는 “같은 제품이라도 소스·빌드·바이너리 생성 시점과 도구에 따라 SBOM 결과가 달라질 수 있다”며, 정답 여부보다는 생성 과정과 방법론의 합리성이 중요하다고 설명했다. NTIA가 제시한 최소 요구사항도 해석이 다양해 국제 표준화가 진행 중이라고 덧붙였다.

김유승 상무는 “처음에는 ‘SCA 도구가 모든 걸 해결해줄 것’이라 생각했지만, 소스코드 기반 스캐너와 패키지 기반 스캐너 모두 한계가 있어 병행해야 사각지대를 줄일 수 있었다”고 언급했다. 그는 규제기관이나 고객과 SBOM 범위·세부 수준을 사전 합의해 혼선을 방지하는 것이 중요하다고 강조했다.

Kevin Fu 교수는 FDA 역시 특정 도구를 강제하지 않으며, 현재 요구사항은 기계 판독 가능한(machine-readable) 형식으로 제출하는 것뿐이라고 설명했다.

Q4. 중소기업이 SBOM/VEX 대응에서 겪는 어려움과 지원 방안은 무엇인가요?

이희조 교수는 “중소기업의 가장 큰 어려움은 인력과 비용”이라며, “완벽한 체계를 한 번에 구축하기보다 내부 시니어 개발자 교육, VDP(취약점 공개 정책) 도입, 오픈소스 보안 도구 활용 등 작은 단계부터 시작할 것을 제안했다.

손미정 팀장은 “식약처는 본질적으로 규제기관이기 때문에 규제 지원 중심으로 역할을 수행한다”며, 새로운 규제가 도입되면 기업이 미리 이해할 수 있도록 안내하고, 컨설팅·설명회를 통해 활용 방법을 제공한다고 설명했다. 법률 문구만으로 이해하기 어려운 부분은 쉽게 풀어낸 가이드라인으로 보완하고 있으며, 2025년 현재 임상 및 사이버보안 분야 규제지원센터를 두 곳 운영 중이고 내년에는 지원 범위를 확대할 계획이라고 덧붙였다.

김유승 상무는 대기업 관점에서 “협력사 소프트웨어를 직접 점검하기 어려워 계약 단계에서 SBOM 제출과 패치 기한 준수 조항을 명시한다”고 소개했다. 또한 “보안 거버넌스가 없는 조직은 우선 핵심 프레임워크·라이브러리 수준에서 ‘승인된 소프트웨어’ 리스트를 정해 관리하는 것이 현실적”이라고 조언했다.

Kevin Fu 교수는 중소기업의 FDA 대응 난이도를 언급하며, “미국에서도 중소 제조사는 품질 시스템과 안전 공학 경험 부족으로 더 많은 검증을 받는다”고 설명했다. 한 제품의 보안 실패는 시장 전체 신뢰 훼손으로 이어질 수 있기에, 대기업이 중소기업 보안 역량을 끌어올리려는 움직임(예: 보안 클리닉, 공동 툴 제공)이 필요하다고 제안하기도 했다.

본 보고서는 과학기술정보통신부·정보통신기획평가원(IITP)의
정보보호핵심원천기술개발 사업 지원을 받아 수행된 연구결과입니다.

- **발행일:** 2025년 9월 26일(금)
- **발행처:** 고려대학교 소프트웨어보안연구소 (CSSA)
  Center for Software Security & Assurance, Korea University
- **홈페이지:** (KOR) https://cssa.korea.ac.kr
  (ENG) https://cssa.korea.edu
- **문의:** cssa@korea.ac.kr