연세대학교
YONSEI UNIVERSITY

CIA Triad 확장모델 및 Threat 모델링에 기반한 소프트웨어 의료기기 사이버보안 프레임워크

연세대학교 대학원

의료기기산업학과

한 혜 리

연세대학교
YONSEI UNIVERSITY

CIA Triad 확장모델 및 Threat 모델링에 기반한 소프트웨어 의료기기 사이버보안 프레임워크

지도교수 구 성 욱 · 장 원 석

이 논문을 석사 학위논문으로 제출함

2025 년 06 월

연세대학교 대학원

의료기기산업학과

한 혜 리

연세대학교
YONSEI UNIVERSITY

CIA Triad 확장모델 및 Threat 모델링에 기반한 소프트웨어 의료기기 사이버보안 프레임워크

한혜리의 석사 학위논문으로 인준함

심사위원장 구 성 욱 (서명)

심사위원 장 원 석 (서명)

심사위원 박 호 준 (서명)

연세대학교 대학원
의료기기산업학과

2025 년 06 월

감사의 글

무더운 여름날 연세대학교 의료기기산업학과 기술사업화 전공으로 입학하여 대학원 생활을 한지 어느덧 2년이라는 시간이 흘러 졸업을 앞두고 있습니다. 소중한 동기들과 처음 만나 함께 부지런히 배우겠다는 의지를 다잡던 입학식 날이 기억이 납니다. 대학원 생활을 하며 큰 도움을 주시고 격려를 아끼지 않았던 모든 분께 감사의 마음을 전하고자 합니다. 특히, 논문을 지도해주시고 심사해주신 구성욱 교수님과 장원석 교수님께 큰 감사의 말씀을 드립니다. 바쁘신 와중에도 논문 작성에 많은 관심과 조언을 해주신 박호준 센터장님께도 감사를 표합니다. 말씀해주신 귀중한 피드백으로 연구의 질을 한층 더 높일 수 있었던 가장 큰 원동력이 되었습니다.

더불어, 석사 과정에서 힘들고 지칠 때 응원과 격려를 서로 아끼지 않아준 이다연 동기님, 유지안 동기님과 김혜민 동기님께도 감사하다는 말씀을 전합니다. 마지막으로 언제나 저의 선택을 지지해주고 믿어주는 제 가족과 사랑하는 연인에게도 항상 사랑하고, 감사하다는 말을 전하고 싶습니다. 이외 도움을 주신 모두에게 감사하다는 말을 다시 한번 드리며, 본 논문이 분야의 학문적 발전에 조금이나마 이바지할 수 있기를 바라며 글을 마칩니다.

2025년 6월

한혜리 올림

차 례

그림 차례

표 차례

국 문 요 약

CIA Triad 확장모델 및 Threat 모델링에 기반한 소프트웨어 의료기기 사이버보안 프레임워크

본 연구를 통해 디지털 헬스케어 시대의 도래와 함께 최근 활용이 급증하고 있는 소프트웨어 의료기기(Software as a Medical Device, SaMD)의 사이버보안 강화를 위한 새로운 접근방식의 사이버보안 프레임워크를 제안하는 것을 목적으로 한다. 최근 의료 분야의 데이터 유출로 인한 평균 피해액이 1,093만 달러에 달하며, 13년 연속 최고치를 기록하는 등 사이버보안 위협이 지속적으로 증가하고 있어 소프트웨어 의료기기(SaMD) 분야에서 사이버보안이 가지는 중요성 및 시급성이 대두되고 있다. 본 연구는 확장된 CIA Triad 모델과 위협 모델링 방법론을 기반으로 소프트웨어 의료기기(SaMD)의 수명주기 전반에 걸쳐 활용할 수 있는 하이브리드 사이버보안 프레임워크(hybrid Cybersecurity Framework, hCSF)를 제안하였다. 본 연구를 통해 제안된 프레임워크는 Parkerian Hexad 모델과 McCumber Cube 모델 등과 같은 확장된 CIA Triad 모델 및 STRIDE, LINDDUN, OCTAVE 등과 같은 다양한 위협 모델링 방법론을 결합하여 기술적, 관리적 및 운영적 측면의 사이버보안 요구사항을 통합적으로 관리할 수 있다. 본 연구를 통한 프레임워크는 Security by Design 원칙을 구현하여 소프트웨어 설계 및 개발 초기 단계부터 보안 요소를 고려함으로써 사후 대응적 접근방식보다 비용 효율적이고, 선제적이며 효과적인 보안체계 구축을 가능하게 할 것이다. 본 연구의 결과, 소프트웨어 의료기기(SaMD)의 의도된 사용 목적, 작용 원리 및 출시 국가의 사이버보안 규제 정책 등에 따라 조직에서 유연하게 다양한 결합형태로 구성한 맞춤형 사이버보안 프레임워크로 활용할 수 있음을 확인하였다. 본 연구는 기존의 기술적 사이버보안 요구사항 체크리스트 방식을 벗어나 소프트웨어 의료기기(SaMD) 수명주기 동안 사이버보안 위협을 식별하고, 위협에 대한 대응전략을 구현할 수 있는 프레임워크를 제안하였으며, 소프트웨어 의료기기(SaMD) 사이버보안 분야에 새로운 이론적 관점과 방향성을 제시하였다. 이를 통해 향후 소프트웨어 의료기기(SaMD)의 글로벌 경쟁력 향상에 도움을 주고, 소프트웨어 의료기기(SaMD)의 사이버보안 프레임워크 정책수립에 기초 연구자료로 활용되어 한층 더 안전하고 신뢰할 수 있는 디지털 헬스케어 및 소프트웨어 의료기기(SaMD)의 사이버보안 관리대책 마련에 기여하고자 한다.

핵심되는 말. 의료기기; 소프트웨어 의료기기; 사이버보안; 위협 모델링 방법론; 프레임워크; 수명주기; CIA Triad; SaMD; Security by Design

1 서론

1.1 연구배경 및 필요성

고령화 및 만성질환의 유병률 증가, 환자맞춤형 의료서비스에 대한 수요 증가 및 클라우드 기반의 서비스형 소프트웨어(Software as a Service, SaaS) 플랫폼의 도입 증가 등과 같은 주요한 동인에 힘입어 디지털 헬스분야 기술의 급속한 발전과 함께 소프트웨어 의료기기(Software as a Medical Device, SaMD)의 활용이 크게 증가하고 있다.[1] 소프트웨어 의료기기(SaMD)는 의료 목적으로 범용 장비에서 사용되는 독립형 소프트웨어를 뜻하며, 일반적으로 진단, 치료 및 모니터링 등 다양한 의료 서비스를 제공한다. 해당 글로벌 시장 규모는 2025년 18억 달러에서 2033년 약 50억 달러의 가치가 있을 것으로 예상되며, 2033년까지의 예측 기간 동안 13.6%의 연평균성장률(Compound Annual Growth Rate, CAGR)로 성장할 것으로 예상된다.[2]

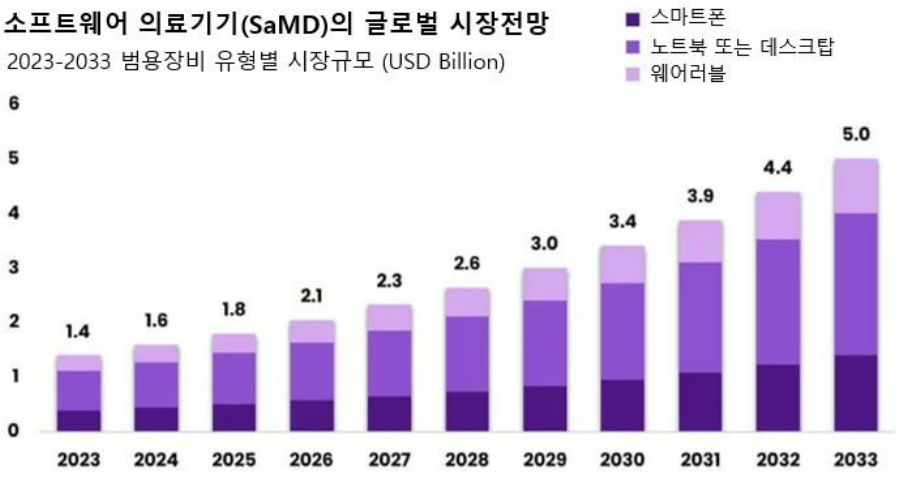

그림 1. SaMD의 글로벌 시장규모 및 성장전망[2]

한편 소프트웨어 의료기기(SaMD)의 확산은 의료데이터 보안 및 개인정보 보호에 대한 우려와 사이버보안 위협에 대한 취약점 증가로 이어지고 있으며, 미국 식품의약국(Food and Drug Administration, FDA)은 2023년 의료기기

사이버보안은 곧 환자 안전이며, 사이버보안 사고는 의료기기의 가용성과 성능에 심각한 위협이 될 수 있음을 시사한 바 있다.[3] 특히 환자 데이터 유출, 무단 접근, 의료기기 기능 변조 등의 사이버 위협이 증가하고 있으며, 이는 환자 안전(Patient Safety)과 직결되는 심각한 문제이다. 또한 국제 의료기기 규제당국자 포럼(International Medical Device Regulators Forum, IMDRF)은 소프트웨어 의료기기(SaMD)의 사이버보안이 제품 수명주기 전반에 걸쳐 고려되어야 할 핵심 요소임을 강조하고 있으나,[4] 현재 지속적으로 발전하고 있는 소프트웨어 의료기기(SaMD)와 사이버 위협을 고려하여 대응할 수 있는 사이버보안 프레임워크는 부족한 실정이다. 기존의 의료기기 사이버보안 가이드라인은 주로 하드웨어를 동반한 종속형 소프트웨어(Software in Medical Device, SiMD)와 혼용되어 개발되거나 기술적 보안 요구사항 체크리스트 방식에 국한되었다는 한계를 가지고 있다.

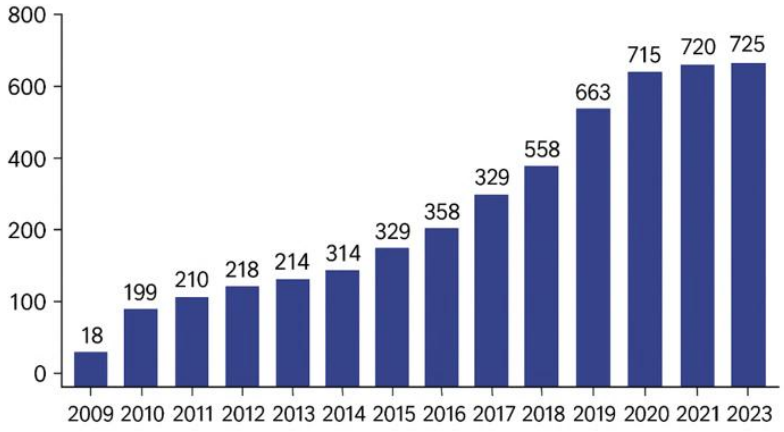

그림 2. 2009-2023년 대규모 의료데이터 침해사례[5]

아울러, 최근 발표된 학술지에 따르면 2023년 의료 분야에서 발생한 대규모 보안침해 사례는 725건으로 보고되었으며, <그림2>에서 확인할 수 있듯이 의료 데이터 침해에 따른 사이버 보안사고가 매년 증가하는 추세이며, 2023년에는 매일 평균 2건의 대규모 의료 데이터 침해가 발생하였다.[5] 시간이 지남에 따라 더욱 정교해지는 사이버 공격에 대처하기 위한 효과적인 방법론의 일환으로 위협 모델링 기반의 소프트웨어 의료기기(SaMD)의 사이버보안 프레임워크를 통한 접근방식은 디지털 헬스분야의 기술 발전에 발맞춘 환자 안전의 확보 및 의료 시스템의 신뢰도 유지를 나아가 산업 및 국가의 경쟁력을 위해 중요한 과제로 대두되고 있다.

1.2 연구 목적

본 연구는 디지털 헬스기술과 함께 증가하는 소프트웨어 의료기기(SaMD)의 사이버보안 위협에 체계적으로 대응하기 위해 확장된 CIA Triad 모델 및 위협 모델링(Threat Modeling) 방법론에 기반한 소프트웨어 의료기기(SaMD)의 사이버보안 프레임워크를 제안하는 것을 목적으로 한다. 먼저, 소프트웨어 의료기기(SaMD)의 특성과 환경을 고려한 잠재적인 사이버보안 위협 요소를 식별하고 분류하며, STRIDE, LINDDUN, OCTAVE, PASTA 및 VAST Threat Modeling 등 다양한 위협 모델링 방법론을 활용하여 새로운 관점의 접근방식을 제시하고, 소프트웨어 의료기기(SaMD)의 수명주기(Life-cycle) 전반에 걸쳐 반복적이고 지속적으로 적용 가능한 맞춤형 사이버보안 프레임워크를 제안하여 제안된 사이버보안 프레임워크의 사례 연구를 통해 적용 가능성을 검토한다. 이를 통해 국내외 사이버보안에 대한 법규 요구사항을 충족하면서도 관련 조직에서 활용할 수 있는 소프트웨어 의료기기(SaMD)의 사이버보안 프레임워크를 제안하고, 소프트웨어의 설계 및 개발 초기 단계부터 사이버보안 위협을 식별하고, 이에 대응할 수 있는 프레임워크를 개발하는 것을 구체적인 목적으로 한다.

본 연구를 통해 제안된 CIA Triad 확장 모델 및 위협 모델링 방법론에 기반한 소프트웨어 의료기기(SaMD)의 사이버보안 프레임워크는 의료기기 분야의 소프트웨어 개발자 뿐만 아니라 이해관계자들이 Security by Design 원칙을 실현할 수 있도록 소프트웨어 수명주기의 초기 단계부터 잠재적인 보안 위협을 구조적으로 식별하고 분석하여 적절한 대응전략을 마련할 수 있도록 지원할 것이다. 이는 소프트웨어 의료기기(SaMD) 분야의 사이버보안 역량 강화에 기여할 뿐만 아니라, 궁극적으로 정보 보안 및 환자 안전을 보장하고 소프트웨어 의료기기(SaMD)에 대한 신뢰성을 확보하는 데 기여할 것이다. 또한, 본 연구의 사이버보안 프레임워크를 통해 국내외 사이버보안 관련 표준 및 규격과 조화를 이루고, 국내 소프트웨어 의료기기(SaMD)의 글로벌 산업 경쟁력 향상에 도움을 주고, 향후 소프트웨어 의료기기(SaMD)의 사이버보안 프레임워크 정책수립에 기초 연구자료로 활용되어 한층 안전하고 신뢰할 수 있는 디지털 헬스케어 및 소프트웨어 의료기기(SaMD)의 사이버보안 관리방안 마련에 조금이나마 기여하고자 한다.

1.3 연구범위 및 방법

1.3.1 연구범위

본 연구는 확장된 CIA Triad 모델 및 위협 모델링에 기반한 소프트웨어 의료기기(SaMD)의 사이버보안 프레임워크를 제안하기 위해 다음과 같은 연구범위를 대상으로 한다. 「의료기기법」 제2조에 해당하는 목적으로 전자·기계장치 등 하드웨어에 결합되지 않고 범용 컴퓨터 등과 동등 환경에서 운영되고 사용되는 독립적인 형태의 소프트웨어와 「디지털의료제품법」의 디지털의료기기 중 전자·기계장치 등 하드웨어에 결합되지 아니하고 범용 컴퓨터 등과 동등한 환경에서 운영되며 그 자체로 디지털의료기기에 해당하는 독립형 디지털의료기기소프트웨어에 적용한다. 특히 유·무선 통신(USB, Wi-Fi, Bluetooth, Ethernet 등)을 사용하거나 외부 시스템과의 통신 경로를 가진 의료기기는 사이버 공격에 더 취약할 수 있으므로 중점적으로 다루며, 소프트웨어 의료기기(SaMD)의 설계 단계부터 개발, 검증, 배포 및 유지보수에 이르는 수명주기 전반에 걸쳐 적용 가능한 방법론을 기반으로 사이버보안 프레임워크를 개발하는 것으로 한정한다. 내장형 소프트웨어 또는 의료기기에도 일부 적용할 수 있으나 전반적인 연구범위에 주요하게 고려하지 않았다.

1.3.2 연구방법

본 연구에서는 확장된 CIA Triad 모델 및 위협 모델링 기반의 소프트웨어 의료기기(SaMD)에 관한 사이버보안 프레임워크를 제안하기 위해 다음과 같은 연구방법을 활용한다. 우선 국내·외 문헌조사를 통해 정보보안 및 사이버보안에 대한 내용을 전반적으로 파악하고, 관련된 국내외 사이버보안 정책자료 및 규제동향을 검토하여 사이버보안 관련 요구사항과 위협 모델링 적용사례 등을 면밀하게 분석한다. 또한, 적용 가능한 대표적인 보안 목표 모델 및 위협 모델링 방법론 등을 수집하고, 수명주기 전반에 걸쳐 사용할 수 있는 프레임워크를 분석 및 제시한다. 현재까지 소프트웨어 의료기기(SaMD) 분야에서 CIA Triad 이외의 보안 모델과 위협 모델링의 적용 사례가 다소 제한적이므로 다양한 분야의 적용 사례를 함께 조사하여 적절하게 조정하는 방안을 모색하도록 한다. 더불어, 의료기기 사이버보안 국제표준 등과의 조화를 위해 국제 의료기기 규제 당국자 포럼(IMDRF)과 국제 표준화 기구(ISO), 국제 전기기술 위원회(IEC) 등과 같은 기관의 관련된 발행자료를 심층적으로 이해하고 적용하여 새로운 프레임워크를 제안하고, 사례 연구를 수행하도록 한다.

2 소프트웨어 의료기기의 사이버보안 프레임워크

2.1 이론적 개념과 원칙

2.1.1 사이버보안의 정의 및 유형

사이버보안(Cybersecurity)에 대한 단일 정의는 존재하지 않고, 각 국가 또는 분야에서 해당 적용 영역에 따라 유연하게 정의하고 사용된다. 미국 연방정부는 국립표준기술연구소(NIST)를 통해 국제적으로 준용되는 사이버보안 분야 표준과 지침을 발행 중이며, 사이버보안을 가용성, 무결성, 인증, 기밀성 및 부인방지를 보장하기 위해 각종 시스템 및 정보를 보호하거나 방어하는 역할로 정의하고 있다.[6] 국내에서는 과학기술정보통신부가 공고한 「정보보호산업의 진흥에 관한 법률(법률 제19990호)」의 정보보호가 유사한 개념으로 정보의 수집, 가공, 저장, 검색 및 송수신 중에 발생할 수 있는 정보의 훼손, 변조, 유출 등을 방지 및 복구하고 암호, 인증, 인식, 감시 등의 보안기술을 활용하여 재난, 재해, 범죄 등에 대응하거나 관련 장비시설을 안전하게 운영하는 것으로 정의하고[7], 의료기기 분야에서는 식품의약품안전처에서 발행한 사이버보안 허가·심사 가이드라인을 통해 IEC TR 60601-4-5:2021 내 용어의 정의를 인용하여 사이버보안을 정보 및 시스템이 인증, 사용통제, 무결성, 데이터 기밀성, 데이터 흐름, 적시 대응 및 가용성과 관련된 위험이 생명주기 내내 허용 가능한 수준으로 유지되는 정도로 접근, 사용, 공개, 방해, 수정 또는 파괴와 같은 인가되지 않은 활동으로부터 보호되는 상태라고 정의하고 있다.[8]

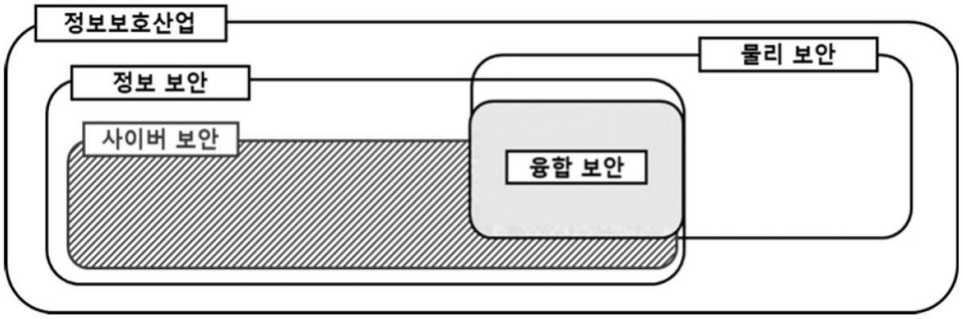

그림 3. 정보보호와 사이버보안의 범위[6]

한편 Microsoft는 사이버보안을 디지털 보안(Digital Security)이라고도 지칭하며, 개인정보, 계정, 파일, 사진, 심지어 돈까지 포함한 디지털 정보, 장치 및 자산을 보호하는 방법이라고 정의하며, AWS는 컴퓨터, 네트워크, 소프트웨어, 애플리케이션, 중요 시스템 및 데이터를 잠재적 디지털 위협으로부터 보호하는 행위로 정의하고, IBM은 컴퓨터 바이러스, 랜섬웨어 공격 등으로부터 개인 및 조직의 시스템 애플리케이션, 컴퓨팅 장치, 민감한 데이터 및 금융 자산을 보호하는 것으로 정의하고 있다. 따라서 사이버보안은 사이버 공격 또는 위협으로부터 데이터, 시스템, 클라우드, 애플리케이션, 엔드포인트 및 네트워크를 보호하는 전반적인 조직의 조치활동을 의미한다. 일반적으로 정보보안 (Information Security)의 맥락에서 사이버보안은 일종의 하위집합으로도 볼 수 있는데, 가장 큰 차이점은 정보보안에서는 디지털과 아날로그를 포함한 모든 데이터를 보호하는 반면, 사이버보안은 주로 디지털 데이터의 안전을 확보하는데 중점을 두고 있다.[6)]

구분	주요 내용
데이터 보안	데이터의 기밀성, 무결성, 가용성을 보호하는 행위를 말한다.
시스템 보안	운영체계(OS), 데이터베이스(DB) 등 컴퓨터 시스템과 관련된 보안에 대한 것으로 악성코드 예방, 백신 소프트웨어 등을 포함한다.
클라우드 보안	클라우드 컴퓨팅 환경에서 데이터 및 서비스를 보호하는 행위를 말한다.
애플리케이션 보안	코드의 취약점을 찾아서 수정해 애플리케이션을 더 안전하게 만드는 행위를 말한다.
엔드포인트 보안	악의적인 내부 및 외부 위협으로부터 데스크톱, 노트북, 서버 및 고정 기능기기를 보호하는 행위를 말한다.
네트워크 보안	승인되지 않은 상태에서 조직 네트워크에 침입하는 것을 차단하거나 방지하는 행위를 말한다.

표 1. 사이버보안의 유형

2.2 사이버 공격, 위협 및 통제

2.2.1 사이버 공격의 유형

사이버 공격(Attack)은 소프트웨어, 네트워크 또는 디지털 장치 등에 무단으로 액세스하여 데이터, 애플리케이션 또는 기타 자산을 도용, 노출, 변경, 비활성화 또는 파괴하는 의도적인 활동을 일컫는다. 일반적으로 개인 또는 조직이 사용하는 컴퓨터 네트워크에서 중요한 문서 및 시스템을 손상시키거나 제어 또는 액세스 권한을 획득하는 데 목표를 두고 개인적, 범죄적 또는 정치적 의도를 가진 개인 또는 조직에 의해 배포된다. 이는 데이터 유출, 운영 중단, 경제적 손실 등을 초래할 수 있으며, 기업 등의 생존과 직결되는 심각한 문제로 부상하고 있다. 최근에는 생성형 AI를 악용해 대량으로 손쉽게 악성코드를 제작하여 사이버 공격을 시도하고 있어 민관협력을 바탕으로 적극적인 대응과 기술 개발이 필요할 것으로 보인다. 일반적으로 가장 널리 통용되는 주요 사이버 공격의 유형은 아래 <표 2>과 같다.[6)]

구분	주요 내용
악성코드 (Malware)	악성 소프트웨어의 줄임말로 컴퓨터 네트워크에 손상을 입히기 위해 고안된 모든 종류의 소프트웨어를 말한다.
피싱 (Phishing)	공격자가 이메일을 조작해 목표 대상을 속여서 어떤 유해한 행동을 취하는 기술을 말한다.
스캠 (Scam)	공격자가 피해자를 속여 민감한 정보를 획득하거나 금전을 갈취하기 위해 신뢰할 수 있는 출처나 인물을 가장하는 공격 방법을 말한다.
랜섬웨어 (Ransomware)	PC의 중요 파일(문서, 사진 등)을 암호화하고 금전을 요구하는 악성코드를 말한다.
서비스 거부 공격 (DDoS)	일부 온라인 서비스가 제대로 작동하지 않도록 시도하는 무작위 입력 공격 방법을 말한다.
중간자 (Man in the Middle)	사이버 범죄자가 사용자와 그들이 접근하려고 하는 웹서비스 사이에 은밀하게 끼어드는 방법을 말한다.

크립토재킹 (Cryptojacking)	다른 사람의 컴퓨터가 공격자를 위해 가상통화를 생성하는 일(가상 언어로 채굴(Mining)이라고 하는 과정)을 하도록 전문화된 공격 방법을 말한다.
SQL 인젝션 (Injection)	공격자가 취약점을 이용해 피해자의 데이터베이스를 제어할 수 있는 수단을 말한다.
제로데이 익스플로잇 (Zero-day exploits)	컴퓨터 소프트웨어의 취약점을 공격하는 공격 방법으로 패치가 나오지 않은 시점에서 이루어지는 공격을 말한다.
공급망 공격 (Supply Chain Attack)	소프트웨어나 하드웨어 공급망을 해킹해 최종 목표를 공격하는 방식을 말한다.

표 2. 사이버 공격(Attack)의 대표적인 유형

사이버 공격은 비즈니스를 방해하고, 피해를 입히고, 심지어 파괴할 수도 있으며, 데이터 침해를 복구하기 위해 발생하는 비용은 평균 435만 달러에 이른다고 한다. 이는 위반을 발견하고 대응하는 데 드는 비용, 다운타임 및 매출 손실, 비즈니스 및 브랜드에 대한 장기적인 평판 손상으로 생기는 손실이 모두 포함된 금액에 해당한다. 특히, 의료 분야는 데이터 유출 등으로 인한 피해 비용 지출이 가장 높으며, 서비스 사업 중단에 가장 취약하여 환자의 안전이 위태로워질 수 있기 때문에 사이버 공격자들의 표적이 되고 있다고 보고된 바 있다.[9)]

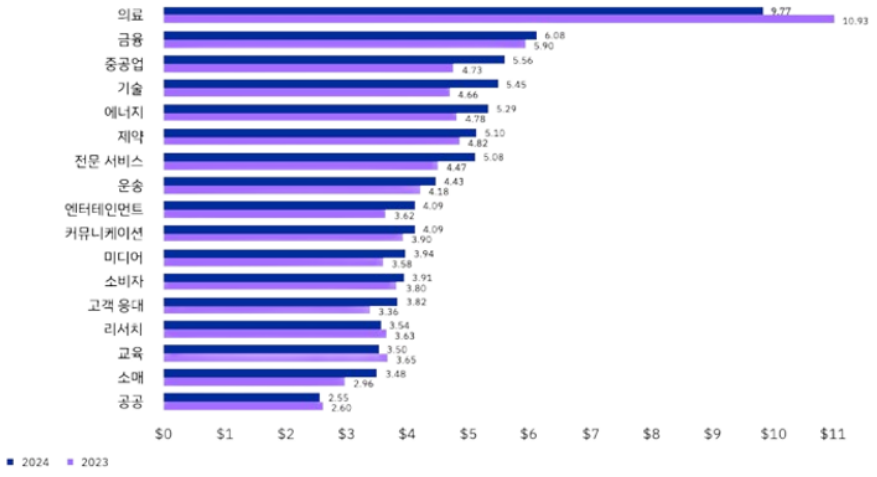

그림 4. 산업별 데이터 유출 비용 발생

2.2.2 사이버 위협의 유형

사이버 위협(Threat)은 개인 또는 조직의 데이터, 정보 및 물리적 자원 등과 같은 자산에 지속적인 위험을 초래하는 사물, 사람 또는 기타 독립체를 일컫는다. 사이버 위협은 항상 존재하며, 의도적이거나 비의도적일 수 있다. 따라서 사이버 공격은 특정 행위가 손실을 초래할 수 있을 때만 존재하는 반면, 사이버 위협은 항상 존재하고 있기 때문에 특정한 보안 상황, 위험에 대한 조직전략 및 자산이 노출 수준을 기반으로 직면한 위협의 우선순위를 정해야 한다. 일반적인 사이버 위협의 주요 유형은 아래 <표 3>과 같다.[10)]

구분	주요 내용
지적 재산권 침해(Compromises to intellectual property)	불법 복제, 저작권 침해 등이 해당한다.
소프트웨어 공격 (Software attacks)	바이러스, 웜, 매크로, 서비스 거부(DoS) 등이 해당한다.
서비스 품질 편차 (Deviations in quality of service)	서비스 제공업체의 ISP, 전원 또는 WAN 서비스 이슈 등 이 해당한다.
첩보 또는 불법침입 (Espionage or trespass)	무단 접근 및/또는 무단 데이터 수집 등이 해당한다.
자연재해(Forces of nature)	화재, 홍수, 지진, 낙뢰 등이 해당한다.
인적 오류 또는 실패 (Human error or failure)	사고, 직원 실수 등이 해당한다.
정보 갈취 (Information extortion)	협박, 정보 공개 등이 해당한다.
누락, 부적절 또는 불완전성 (Missing, inadequate, or incomplete)	백업 및 복구계획, 조직 정책/계획 없이 드라이브 장애로 인한 정보 시스템 접근권한 상실 등이 해당한다.
누락, 부적절 또는 불완전한 통제(Missing, inadequate, or incomplete controls)	방화벽 보안제어 부재로 인한 네트워크 손상 등이 해당한다.
사보타주 또는 기물파손 (Sabotage or vandalism)	시스템 또는 정보 파괴 등이 해당한다.

절도(Theft)	장비 또는 정보의 불법적 몰수 등이 해당한다.
기술적 하드웨어 실패 또는 오류(Technical hardware failures or errors)	장비 고장 등이 해당한다.
기술적 소프트웨어 실패 또는 오류 (Technical software failures or errors)	버그, 코드 문제, 알려지지 않은 허점 등이 해당한다.
기술적 노후화 (Technological obsolescence)	시대에 뒤떨어지거나 구식인 기술 등이 해당한다.

표 3. 사이버 위협(Threat)의 주요 유형

또한, 미국 식품의약국(FDA)에 따르면 사이버 위협은 소프트웨어를 통해 의료기기, 기업 운영(임무, 기능, 이미지 또는 평판 포함), 기업 자산, 개인 또는 기타 조직에 무단 접근, 파괴, 공개, 정보 수정 또는 서비스 거부를 통해 부정적인 영향을 미칠 가능성이 있는 모든 상황 또는 사건이라고 정의한다. 사이버 위협은 일반적으로 의료기기의 안전성 또는 유효성에 영향을 미칠 수 있는 취약점을 활용하므로 소프트웨어 의료기기(SaMD) 제조회사는 소프트웨어의 설계 및 개발 초기 단계에서 자산으로부터 취약점을 제거하고, 자산에 대한 접근을 제한하며, 보호 조치를 추가해야 한다.[11)]

2.2.3 보안 통제의 유형

미국 식품의약국(FDA)에 따르면 보안 통제(Security Control)를 통해 무결성을 포함한 진위성, 승인, 가용성, 기밀성 및 시기적절한 업데이트 가능성 등과 같은 사이버보안 목표를 달성할 수 있으며, 보안 중심의 제품 개발 프레임워크(Secure Product Development Framework, SPDF)의 필수 요소라고 밝혔다. 일반적으로 <표 4>와 같이 인증, 권한 부여, 암호화 등과 같은 보안 통제를 권장하고 있으며, 단, 이에 국한되지는 않는다.[11)]

구분	주요 내용
인증 (Authentication)	암호화 기반 인증 사용, 다단계 인증, 강력한 키 관리, 물리적 신호 기반 승인 구현, 재전송 방지, 하드코딩 또는 기본 비밀번호 사용금지 등이 해당한다.
권한 부여 (Authorization)	역할 기반 권한 모델, 기본 거부 설계, 세션시간 제한, 근접신호 기반 승격권한 허용 등이 해당한다.
암호화 (Cryptography)	표준 권장 알고리즘 사용, 다운그레이드 방지, 공개 정보로 키 생성금지 등이 해당한다.
코드, 데이터 및 실행 무결성(Code, Data, and Execution Integrity)	디지털 서명 사용, 외부 데이터 범위 및 프로토콜 검증, 테스트 또는 디버그 포트제한 등이 해당한다.
기밀성 (Confidentiality)	암호화로 저장 또는 전송 데이터 보호, 자격증명 보호, 위험 기반 시스템 설계, 등이 해당한다.
이벤트 탐지 및 로깅 (Event Detection and Logging)	보안 이벤트 로깅 및 타임스탬프, 로그 외부 저장 및 문서화, 네트워크 이상 등 탐지, SBOM 자동생성 기능 고려 등이 해당한다.
복원력 및 복구 (Resiliency and Recovery)	프로세스 격리 또는 가상화, 신뢰 실행 환경 활용, 네트워크 중단 또는 DoS 복원력 설계 등이 해당한다.
펌웨어 및 소프트웨어 업데이트(Firmware and Software Updates)	보안 업데이트 위한 리소스 확보, 다운타임 대비 설계, 사이버보안 패치 프로세스 분리, 테스트 또는 빌드 환경 유지, 타사 소프트웨어 라이선스 관리 등이 해당한다.

표 4. 보안 통제(Security Controls)의 주요 유형

2.2.4 의료기기 사이버보안 요구사항

의료기기 사이버보안 요구사항과 관련하여 미국 FDA와 유럽 EU 등의 경우 사이버보안을 단순한 기술적 요구사항이 아닌 전 주기적인 품질경영시스템의 일부로 고려하고 있으며, 설계 및 개발단계에서부터 시판 후 단계까지 전 주기적으로 관리할 것을 요구하고 있다.[11)12)] 한편, 국내 식약처는 사이버보안 침해로 인한 위해도, 통신방법 및 사용환경을 고려하여 사이버보안 규제의 국제조화를 위해 IEC 62443-4-2:2019 등과 같은 규격을 적용하며, 현재 사용되는 의료기기의 특성을 반영한 7가지 기술적 요구사항을 허가·심사 시 충족하도록 요구하고 있다.

구분	상세 요구사항
식별 및 인증 (Identification and Authentication)	사용자 식별 및 인증, 계정 관리, 식별정보 관리, 인증정보 관리, 비밀번호 강도 설정, 인증정보에 대한 피드백, 연속적인 로그인 시도 실패 시 로그인 제한 및 시스템 사용 알림 메시지 등이 요구된다.
사용 통제 (Use Control)	권한 부여, 모바일 코드 사용 통제, 세션 잠금, 감사기록 생성, 감사 처리 실패 대응, 타임스탬프, 부인 방지 등이 요구된다.
시스템 무결성 (System Integrity)	통신에 대한 무결성 보장, 악성코드로부터 보호, 보안 기능 검증, 소프트웨어 및 정보에 대한 무결성 점검, 입력값 검증, 오류 시 사전 결정된 상태로 출력, 오류 처리, 업데이트, 업데이트에 대한 진본성 및 무결성 검증, 물리적 변조 방지, 부트 프로세스 무결성 검증 등이 요구된다.
데이터 기밀성 (Data Confidentiality)	정보에 대한 기밀성 보장, 보건의료정보 비식별화, 안전한 암호화 사용 등이 요구된다.
이벤트 적시대응 (Timely Response to Events)	감사로그에 대한 비인가된 접근 제한 등이 요구된다.
자원 가용성 (Resource Availability)	서비스 거부(Denial of Service, DoS) 방지, 의료기기 백업, 의료기기 복구 및 재구성, 네트워크 및 보안 구성 설정, 불필요한 기능 비활성화 등이 요구된다.

표 5. 국내 의료기기 사이버보안 요구사항

적용이 어려운 요구사항은 미적용 사유를 입증하는 자료를 제출해야 하며, 의료기기 특성이나 기술 변화에 따라 요구사항이 추가 또는 제외될 수 있다. 식약처는 제품 허가 후에도 이러한 사이버보안 요구사항을 지속적으로 관리하도록 요구하고 있으며, 추가적으로 해당하는 경우, 인공지능 보안 관련 지침에 따라 검증해야 한다.[8] 한편, 국제 의료기기 규제당국자 포럼(IMDRF)은 효과적인 사이버보안 요구사항 관리를 위해서는 <그림5>과 같이 개발 단계, 지원 단계, 제한적 지원 단계 및 지원종료 단계를 아우르는 제품수명 전 주기(Total Product Life Cycle, TPLC) 프레임워크를 통해 사이버보안 위협 및 취약성과 관련된 위험을 모든 단계에 걸쳐 고려해야 하고, TPLC 동안 환자 피해의 위험을 최소화할 수 있도록 의료기기 제조업체(Medical Device Manufacturers, MDM), 의료서비스 제공자(HealthCare Providers, HCP), 사용자, 규제기관 및 취약점 발견자를 포함한 모든 이해관계자가 사이버보안을 공동책임으로 인식하고, 사이버보안 사고와 위협 및 취약점에 대비하는 광범위한 정보공유 정책을 추진하고 투명성을 높이며 대응하는 방안을 권장하고 있다.[13)14)]

그림 5. IMDRF의 사이버보안 제품수명 전 주기 프레임워크

2.3 국내외 사이버보안 정책 및 규제

사이버보안은 정보보호와 관련된 법규, 정보통신기반보호법, 개인정보보호법 등의 제·개정에 크게 영향을 받는 국가 정책에 민감한 분야이며, 사회의 주요한 이슈에 영향을 받는 기술 분야에 해당한다. 최근 국가와 기업의 보안을 위협하는 국제적인 해킹조직의 증가와 빈번해진 데이터 유출사고 등으로 인해 전 세계적으로 사이버보안 관련 법률 및 정책을 강화하는 추세이며, 사이버보안 분야의 중요성과 사회적 관심이 지속적으로 높아지고 있다.

2.3.1 국제 사이버보안 관련 동향

(1) 미국(United States)

미국 연방정부는 최근 정치적 변화, 기술발전과 지속적인 보안위협 증가에 대응하여 국가 차원의 사이버보안 정책을 강화하고 있다. 2023년 National Cybersecurity Strategy에서는 사이버보안 책임의 분산구조에서 벗어나 개발업체와 공급업체에게 보다 명확한 책임을 부여하는 방향으로 정책기조를 전환하였고, 소프트웨어 공급망의 투명성 확보, 취약점 대응체계 정비, 보안 업데이트 및 지속적인 모니터링 등을 핵심 과제로 제시하였다. 또한, 행정부 2기 이후 미국 정부는 공격적 보안전략을 표방있으나, Cybersecurity and Infrastructure Security Agency에 대한 예산삭감, 고위인사의 이탈 및 자문기구 해체 등으로 인해 실질적인 사이버 방어역량은 약화되고 있다는 지적이 제기되고 있다. Department of Government Efficiency는 인공지능(AI) 기반의 시민 데이터 중앙화 정책을 추진하고 있으며, 관련된 개인정보 보호와 국가안보 침해 우려도 커지고 있는 상황이며, 이를 타개하고자 산업계와의 협력을 통해 사이버보안 대응역량을 강화하고자 실리콘밸리 현장 청문회 등 정책적 연계를 추진하고 있다.[7)18)]

한편, 의료기기 분야에서는 미국 FDA가 사이버보안을 환자의 안전과 직결되는 핵심 요소로 고려하여 의료기기 제조업체를 대상으로 점차 더욱 강화된 보안 요구사항을 요구하고 있다. 2022년 12월 Consolidated Appropriations Act, 2023의 일부로 Food and Drug Omnibus Reform Act of 2022 법안이 통과됨에 따라 Federal Food, Drug, and Cosmetic Act (FD&C Act) 제524B조가 신설되었으며, 일명 사이버 디바이스(Cyber Device)로 분류되는 의료기기에 대해서는 보안 업데이트, 위협

모델링 등을 활용한 취약점 대응계획, 소프트웨어 구성요소 명세서(SBOM)의 제출 등 보안관리 체계수립이 법적으로 의무화되었다. 나아가 FDA는 2023년 9월에 최종 발간한 Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions을 발표하며, 사전 인허가 과정에서 요구되는 사이버보안 문서의 구체적 기준을 제시하였다. 특히 2024년부터 본격적으로 시행된 electronic Submission Template And Resource(eSTAR)를 통해 사이버보안 요건이 충분히 충족되지 않을 경우 해당 기기의 허가 자체가 거부될 수 있게 되었으며, FDA는 개발 초기단계부터 보안을 고려할 수 있도록 전 수명주기에 걸친 Security Product Development Framework(SPDF)의 적용을 권고하고 있다.[15)19)20)]

(2) 유럽연합(European Union, EU)

유럽 연합(EU)은 디지털 전환 가속화 및 사이버 위협이 고도화됨에 따라 전면적으로 사이버보안 정책을 강화하고 있다. 유럽은 다수의 입법조치를 통해 디지털 제품 및 서비스 전반에 걸친 보안성 확보를 목표로 하고 있으며, 의료기기를 포함한 기술기반 산업에 중요한 규제적 영향을 미치고 있다. 우선 2024년 10월부터 시행된 Network and Information Systems Directive 2는 에너지, 금융, 보건의료 등 핵심 인프라를 포함한 다양한 부문에 대해 사이버보안 관리 체계 구축, 사고대응 계획수립, 정보공유 및 보고체계 강화 등을 법적으로 요구하고 있다. 이 지침은 EU 회원국들이 이를 국내법에 통합하여 이행하도록 규정하고 있으며, 의료기관과 의료기기 제조업체도 주요 적용 대상에 포함된다. 한편, Cyber Resilience Act는 디지털 요소가 포함된 모든 제품에 대해 생애주기 전반에 걸쳐 사이버보안 요건을 의무화하는 사이버 복원력 법안으로 2024년 말 채택되어 단계적으로 시행되고 있다. 해당 법안은 제조업체에게 제품 개발 초기 단계부터 보안을 고려한 설계를 의무화하며, 출시 이후에도 보안 업데이트 제공, 취약점 보고, 위험 평가 등을 지속적으로 수행할 것을 요구한다. 이는 의료기기와 같이 지속적으로 연결되는 디지털 제품의 안전성과 신뢰성을 높이는 데 중대한 기반을 제공한다. 이와 더불어, 2025년 1월부터 시행된 Digital Operational Resilience Act는 금융 산업을 대상으로 하나, ICT 리스크 관리 전반을 포괄하는 규정으로 의료정보 처리기관에도 간접적인 영향을 미칠 수 있다. 특히 EU는 Cyber Solidarity Act를 통해 회원국 간 사이버 위협에 대한 공동 대응 체계를 구축하고 있으며, 유럽 차원의 사이버보안 경보 시스템 운영을 추진 중이다.[7)21)]

한편, 의료기기 분야의 경우 Cyber Resilience Act와 Network and Information Systems Directive 2의 중첩적 적용으로 인해 제품의 전 주기에 걸쳐 보안성 확보가 요구된다. 아울러, EU는 사이버보안 인증 체계를 도입하여 ICT 제품 및 서비스의 보안 수준을 객관적으로 평가하고 있으며, 이는 의료기기 등 고위험 제품의 시장 진입 및 신뢰성 확보에 중요한 요소로 작용하고 있다. 2017년에 발효된 Medical Device Regulation (MDR)은 사이버보안을 안전성과 성능 요구사항 중 하나로 명시하고 있으며, MDR 제17조는 소프트웨어의 설계 및 제조가 최신 기술을 반영해야 한다고 규정하고 있다. MDR 부록 I에서는 사이버보안 위험이 수반되는 기기에 대해 일반 안전 및 성능 요건(General Safety and Performance Requirements, GSPR)을 구체적으로 제시하고 있으며, 2020년 개정한 MDCG 2019-16 Guidance on Cybersecurity for medical devices을 통해 사이버보안과 관련된 위험 식별, 보안통제의 적용, 검증 및 테스트, 그리고 시판 후 모니터링 등을 포함하고 있으며, 보안 요구사항의 추적성과 일관성을 확보하는 데 중점을 두고 있다.[12)]

(3) IMDRF (International Medical Device Regulators Forum)

IMDRF는 의료기기 사이버보안의 국제적 기준 정립을 위해 2020년 Principles and Practices for Medical Device Cyber security를 발행하여 의료기기의 전 생애주기(Total Product Life Cycle, TPLC)에 걸친 사이버보안 접근을 제시하였으며, 의료기기 제조회사, 의료기관 및 환자 등 다양한 이해관계자 간의 역할과 책임을 명확히 하였다. 특히, 정보 공유, 위험 기반 설계, 보안 패치 관리, SBOM(Software Bill of Materials) 도입 등을 통해 보다 체계적인 사이버보안 관리체계를 강조하였다. 이후 2023년 Principles and Practices for the Cybersecurity of Legacy Medical Devices (IMDRF/CYBER WG/N70)에서 사이버보안 설계가 미흡하거나 업데이트가 불가능한 레거시(legacy) 의료기기에 대한 보안 위험 평가 및 관리 전략을 제시한다. 레거시 기기의 정의를 명확히 하고, 제조사와 의료기관 간의 협력적 보안 유지 방안을 규정함으로써 기존 의료기기의 사이버보안 강화를 위한 기준점을 제공하고 있다. 또한, 2023년 Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity (IMDRF/CYBER WG/N73)를 통해 의료기기 소프트웨어의 구성요소에 대한 투명성 확보를 위해 SBOM의 정의, 구성요소, CycloneDX, SPDX 등과 같은 형식 및 적용 사례를 상세히 설명하고 있다. 이를 통해 사이버 위협 대응 시 소프트웨어 구성 정보에 기반한 신속한 취약점 식별과 보안

유지보수가 가능하도록 지원한다. IMDRF의 사이버보안 지침은 글로벌 의료기기 생태계 전반에서 보안 관리 수준 향상과 규제 조화 촉진에 기여하고 있다.[4)13)14)]

2.3.2 국내 사이버보안 관련 동향

국내에서는 2022년 5월 사이버보안을 주요 국정과제로 채택하고, 범정부차원의 협력체계 공고화, 기술패권 대응, 산업기술 인재 경쟁력 제고 등의 정책을 도입하였다. 「사이버 10만 인재 양성방안(2022.07)」, 「대한민국 디지털 전략(2022.09), 「국가전략기술 육성방안(2022.10)」 및 「정보보호산업의 글로벌 경쟁력 확보전략(2023.09)」 등과 같은 다양한 정보보호 관련정책을 수립하여 지속적으로 마련하고 있으며, 정보보호 공시제도 의무화('21.12), 신속확인제 도입('22.11), 개인정보보호법 전면개정 및 정보보호관리체계(Information Security Management System, ISMS) 인증제도 확대시행 및 글로벌 공략을 위한 생태계 확충 등 적극적인 제도시행으로 기업의 시장진입 애로를 해소하고, 정보보호 투자촉진을 유도하고 있다. 특히 과학기술정보통신부가 2022년 10월 발표한 「국가전략기술 육성방안」을 통해 사이버보안을 12대 국가전략기술로 지정하고, 국가 경쟁력 강화를 위해 중점적으로 육성하고자 하는 핵심분야로 제시하여 민관협동으로 산업혁신 전략을 추진 중이다.[6)7)22)]

한편, 의료기기 분야에서는 최근 식품의약품안전처가 2025년 1월에 의료기기의 사이버보안 허가·심사 가이드라인을 5차 개정하여 발행하였고, 「디지털의료제품법」 제정에 따른 적용범위 명확화와 IEC 62443-4-2, IEC TR 60601-4-5 국제규격 및 기술적 특성을 반영한 사이버보안 요구사항의 시행시기를 명확화했다. 2025년 6월 30일까지 한시적으로 개정 전의 사이버보안 요구사항을 적용한 검증 자료를 제출할 수 있도록 하고 있으며, 디지털의료기기에 한하여 「디지털의료제품법」의 시행일인 2025년 1월 24일부터 적용하여 인공지능 보안에 대한 추가 검증을 포함한 제출 자료를 요구하고, 「디지털의료제품법」 제14조, 제32조 및 같은 법 시행규칙 제29조 제2항 등에 따른 전자적 침해행위 보호규정을 통해 DDoS 공격, 데이터 유출, 해킹 등 디지털의료기기 및 그 운영환경을 공격하는 행위에 관한 보안정책, 취약점 조치방안 및 침해사고 대응방안 등과 같은 준수사항을 마련하였다.[8)23)]

3 CIA Triad 확장모델 및 위협모델링 개요

3.1 CIA Triad 및 확장모델

CIA 트라이어드(Triad)는 대표적인 정보보안의 3대 원칙을 나타내며, <그림6>과 같이 기밀성(Confidentiality), 무결성(Integrity) 및 가용성 (Availability)으로 구성되어 있다. CIA 트라이어드는 1972년 앤더슨(Anderson) 보고서를 통해 제시되었으며, 이후 Saltzer와 Schroeder 등과 같은 학자들에 의해 이론적으로 체계화되었다. 먼저, 기밀성은 인가된 사용자만 정보에 접근할 수 있도록 보장하는 원칙 또는 정보가 승인되지 않은 개인, 조직 또는 프로세스에 노출되거나 이용 가능하지 않도록 하는 속성을 말한다. 둘째, 무결성은 정보의 정확성과 완전성을 유지하는 원칙 또는 정보가 부적절하게 변경되거나 파괴되지 않도록 보장하는 속성을 의미한다. 마지막으로 가용성은 필요한 시점에 정보를 적시에 접근할 수 있도록 하는 원칙 또는 권한 있는 개체가 접근하고 사용할 수 있는 속성으로 규정한다.[11)15)]

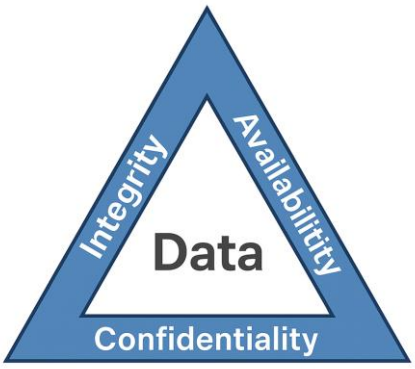

그림 6. CIA Triad의 3대 원칙

국내 식약처의 경우, 의료기기의 사이버보안 허가·심사 가이드라인을 통해 의료기기 사이버보안 기본원칙으로 이를 명명하고 있으며[8)], CIA 트라이어드는 본 연구의 제3장에서 소개할 위협 모델링 방법론과 결합될 때 소프트웨어 의료기기(SaMD)의 효과적인 사이버보안 프레임워크를 위한 근본적인 기반을 제공할 수 있다. 한편, CIA트라이어드만으로는 끊임없이 변화하는 새로운 기술, 비즈니스 요구사항 및 복잡한 위협환경에 대응하기에 한계가 존재한다는 지적이 계속되고

있으며, 이러한 한계점을 보완할 수 있는 더욱 강력한 보안목표 모델의 개발을 촉진시켰고, 다양한 대안 모델 또는 확장 모델이 제안되었다. 대표적인 확장된 CIA Triad 모델에는 Parkerian Hexad 모델과 McCumber Cube 모델 등이 있다. Parkerian Hexad 모델은1998년 Donn B. Parker가 제안한 6가지 보안 요소로 구성된 모델이며, 고전적인 CIA 트라이어드에 소유 또는 통제(Possession or Control), 진위성(Authenticity)과 유용성(Utility)을 추가하여 속성을 한층 더 정교하게 확장하였다. Parkerian Hexad 모델은 보안 요소를 단순히 기술적 요소에 한정하지 않고, 현실적인 보안 사고 시나리오까지 포괄하는 특징을 가지고 있어 한층 다각도로 사이버보안을 평가할 수 있으며, 보안 정책 수립, 보안 사고 분석 및 위협 식별에 있어 보다 정교한 기준을 제공한다.[10)16)17)]

그림 7. McCumber Cube 모델

특히 McCumber Cube모델은 1991년 John McCumber가 제시한 3차원의 보안 모델로서 <그림7>과 같이 보안 목표, 정보 상태 및 보안 대책의 원칙이 x, y, z 축을 기준으로 입체적으로 구성되어 있고, 총 27개의 보안 요소에 관한 분석을 통해 보안 위협 또는 취약점을 다각도로 평가하고, 대응하기 위한 대책을 수립하고 시각화할 수 있어 모든 유형의 조직에서 보안 정책 수립, 위험 평가 및 교육 및 감사 등 다양한 분야에서 활용할 수 있다.[10)]

3.2 위협모델링 방법론 개요 및 종류

3.2.1 Threat Modeling 정의 및 특징

위협 모델링(Threat Modeling)은 소프트웨어의 잠재적인 위협과 취약점을 보다 체계적으로 식별하고 분석하기 위한 구조화된 접근방식이자 프로세스 방법론으로써 소프트웨어 수명주기의 초기 단계부터 효과적인 사이버보안 대응방안을 설계하기 위한 기반을 제공해준다. 위협 모델링 방법론을 전략적으로 활용하면 소프트웨어에 대한 추상화, 잠재적 공격자의 목표 및 수법을 포함한 프로필 및 발생가능한 잠재적 위협목록을 작성함으로써 위협과 대응방안을 효과적으로 파악할 수 있기 때문에 집중적인 방어를 할 수 있는 소프트웨어 아키텍처를 설계할 수 있다. 현재 기업들이 활용할 수 있는 수많은 위협 모델링 방법론 또는 방법론이 존재하는데, 일부 방법은 추상화와 세분화에 중점을 두고, 일부는 사람 중심적인 접근방식을 취하며, 나머지는 위험이나 개인정보보호에 관한 이슈사항에 초점을 맞춘 방법도 있다. 이러한 위협 모델링을 2가지 이상 결합하여 잠재적 사이버 위협에 대해 더욱 강력하고 다각적인 관점을 제안하고 활용할 수도 있다.[24)]

일반적으로 위협 모델링 방법론을 가장 효과적으로 활용하기 위해서는 소프트웨어 수명주기의 개발초기 단계에서 선제적으로 수행하는 것이 권장하고 있으며, 이는 광범위한 유형의 사이버 위협을 식별하고 조기에 잠재적 위협을 발견하여 해결할 수 있어 추후 비용이 훨씬 많이 소요될 수 있는 보안과 관련된 품질비용을 예방하기 위함이라고 볼 수 있다. 단, 위협 모델링 방법론을 선택하는 경우 특정한 위협 모델링 방법론이 다른 기법보다 더욱 권장되는 것은 아니며, 어떤 위협 모델링 방법론을 사용할지는 프로젝트의 요구사항과 우려사항 등을 충분히 고려하여 결정해야 한다. 소프트웨어 의료기기(SaMD)와 관련하여서는 미국 FDA가 2023년 9월 Cyber security in Medical Devices: Quality System Considerations and Content of Premarket Submissions라는 가이던스를 발행함으로써 위협 모델링을 활용하여 사이버보안에 관한 시판 전후의 위험관리 프로세스를 수행할 것을 적극적으로 권장하고 있다.[11)24)]

3.2.2 STRIDE 위협 모델링

STRIDE 위협 모델링은1999년 Loren Kohnfelder와 Praerit Garg가 고안했으며, 2002년 Microsoft사에 의해 도입되어 현재 가장 널리 사용되는 위협 모델링 방법론이다. 위장(Spoofing), 변조(Tampering), 부인(Repudiation), 정보 유출(Information Disclosure), 서비스 거부(Denial of Service) 및 권한 상승(Elevation of Privilege)과 같은 6가지 위협 범주를 적용하여 보안 취약점을 식별한다. STRIDE 위협 모델링은 비교적 직관적인 구조를 가지고 있어 소프트웨어 설계의 초기 단계에서 활용하기에 적합하며, 공격자 관점에서 소프트웨어를 분석함으로써 잠재적인 위협을 파악하는데 용이하다는 장점을 가지고 있다. 위협 별 테이블과 STRIDE-per-Element, STRIDE-per-Interaction과 같은 버전을 포함하면서 발전해왔고, 소프트웨어의 세부적인 설계를 평가하는데 활용할 수 있다.

	위협	자산	위반된 위협에 대한 정의
S	Spoofing identify	Authentication	본인이 아닌 다른 사람 또는 사물로 가장함
T	Tampering with data	Integrity	네트워크, 메모리 또는 기타 위치에서 데이터를 수정하거나 변조함
R	Repudiation	Non-repudiation	자신이 어떤 행위를 하지 않았거나 책임이 없다고 주장함
I	Information disclosure	Confidentiality	접근 권한이 없는 사람에게 정보를 제공하거나 공개함
D	Denial of service	Availability	서비스 제공에 필요한 자원이 고갈됨
E	Elevation of privilege	Authorization	권한이 없는 사람에게 작업을 수행할 수 있도록 허용함

그림 8. STRIDE 위협 모델링의 핵심 개요

우선, 데이터 흐름도(Data Flow Diagram, DFD)을 작성함으로써 소프트웨어의 구성요소, 이벤트 및 경계 등을 식별할 수 있고, DFD는 STRIDE 위협 모델링의 성공적인 활용을 결정짓는 핵심요소이다. 다만, DFD만을 유일한 입력사항으로 사용하면 보안 관련 아키텍처 요구사항을 결정하는데 한계가 있다. 둘째, 상기 6가지 위협 범주를 사용하여 위협을 식별하고, 식별된 위협과 각 위협에 대한 대응방안을 수집하여 문서화하고 우선순위를 정해야 한다. STRIDE 위협 모델링은 도입이 비교적 쉬우나 소프트웨어가 복잡해질수록 위협의 수가 급격히 증가하고 시간이 많이 소요된다는 단점을 가지고 있다. Scandariato 등에 따르면 STRIDE는 거짓 양성율이 비교적 낮지만, 거짓 음성률은 비교적 높다고 보고된 바 있으며, Microsoft사는 현재 STRIDE를 더 이상 공식적으로 유지 및 관리하지 않지만, Threat Modeling Tool을 통해 Microsoft Secure Development Lifecycle의 일부로 여전히 구현하고 있다.[25)]

3.2.3 LINDDUN 위협 모델링

LINDDUN위협 모델링은 2010년 벨기에 Katholieke Universiteit Leuven 대학에서 발표하고, 꾸준히 학계와 업계 파트너와의 긴밀한 협력을 통해 개선하여 2023년 새롭게 수정된 버전을 출시한 방법론이다. LINDDUN 위협 모델링은 특히 개인정보 보호분야에 중점을 두고 있으며, 데이터 보안을 위해 활용하기 적합하다. 연결성(Linkability), 식별성(Identifiability), 부인 방지(Non-repudiation), 탐지성(Detectability), 정보 공개(Disclosure of information), 인식 부족(Unawareness), 규정 미준수(Non-Compliance)와 같은 7가지 위협 범주에 대해 <그림9>와 같은6단계의 프로세스를 따른다. LINDDUN은 개인정보 보호평가를 위한 체계적인 접근방식을 제공하고, 데이터 흐름도(DFD)을 작성하는 것부터 시작한다. 모든 구성요소를 체계적으로 반복하면서 각 요소를 위협 범주의 관점에서 분석하고, 해당 위협이 소프트웨어에 어떻게 적용될 수 있는지를 식별하며 위협 트리를 구성한다.

그림 9. LINDDUN 위협 모델링의 핵심 개요

또한 2단계와 3단계는 본질적으로 소프트웨어의 위협을 식별하는 초기 분석 과정을 안내하는 일종의 설문 형식이며, 2단계에서는 각 위협 범주가 소프트웨어의 어떤 부분에서 발생할 수 있는지를 매핑하고, 3단계에서는 해당 위협이 실제로 발생할 수 있는 위협 시나리오를 파악한다. 이후 프로세스 단계에서는 위협에 대한 해결 방안과 완화 전략을 제안하게 된다. LINDDUN의 장점 중 한 가지는 방대한 개인정보 보호분야와 관련된 지식기반의 문서화가 잘 되어 있다는 부분이지만, 적용 시 많은 작업량과 시간이 요구되며 STRIDE 위협 모델링과 마찬가지로 소프트웨어가 복잡해질수록 위협의 수가 급격히 증가하는 한계점이 있다.[25)]

3.2.4 OCTAVE 위협 모델링

OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) 위협 모델링은 카네기 멜론 대학교의 소프트웨어 공학 연구소(Software Engineering Institute, SEI) 산하 CERT 부서에서 개발하였으며, 특히 조직 차원의 위협, 자산 및 취약점 평가에 중점을 둔다. 기술적 위험 중심의 일반적인 위협 모델링 방법론과 다르게 조직적 위험을 목표로 하고, 전략적 실무관련 문제에 초점을 맞출 수 있어 조직의 정보보안 거버넌스 및 정책 수립에 효과적으로 적용할 수 있다. OCTAVE는 운영 리스크, 보안 관행 및 기술이라는 3가지 핵심요소에 기반을 두고, 자산 기반의 위협 프로파일을 구축하는 조직평가 단계, 정보 인프라의 취약점을 식별하고 평가하는 기술평가 단계 및 조직의 핵심자산에 대한 위험식별 및 전략개발 단계로 구성되어 있으며, 연속적인 프로세스가 아닌 개별적인 활동을 평가한다.

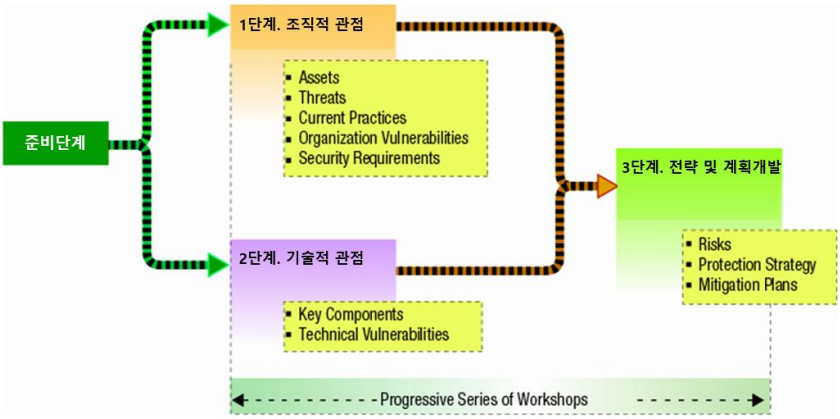

그림 10. OCTAVE 위협 모델링의 핵심 개요

OCTAVE는 주로 대규모 조직을 위해 설계되었으나, 소규모 조직을 위해 설계된 OCTAVE-S 방법도 제공한다. 자산식별 및 정보보호 위험평가를 주도적으로 접근하는 방식이므로 심층적이면서도 유연한 방법론을 제공하지만, 많은 시간적 투자가 필요하고, 문서화가 방대하며 다소 모호하다는 한계가 있다. 이러한 부분을 개선하기 위해 2007년에 OCTAVE Allegro을 개발하여 자원과 전문적인 지식이 부족할 수 있는 소규모 조직이 활용할 수 있도록 보다 간소화되고 최적화된 위협 모델링 방법론을 제시하기도 했다.[25)]

3.2.5 PASTA 위협 모델링

PASTA (Process for Attack Simulation and Threat Analysis) 위협 모델링은 2012년 Tony UcedaVelez가 개발한 공격 시뮬레이션 기반의 접근방식으로 총 7단계에 걸쳐 조직의 비즈니스 목표 정의부터 공격 시나리오 분석, 위험평가에 이르기까지 포괄적인 분석 프로세스를 제공한다. 실제 발생 가능한 위협 시나리오와 공격자를 식별 및 분석하고, 소프트웨어 내 취약점을 위협과 연계하여 평가하여 이에 대한 대응 또는 완화 전략을 수립한다. 특히, 공격자의 관점에서 위협을 시뮬레이션함으로써 실질적인 공격 가능성과 영향을 평가할 수 있어 고도화된 위협분석이 요구되는 환경에서 유용하다. PASTA는 비즈니스 목표와 기술적 요구사항을 통합하는 것을 목표로 하고, 각 단계에서 다양한 설계 및 제안 도구를 사용한다.

그림 11. PASTA 위협 모델링의 핵심 개요

6단계에서는 분석 및 공격 모델링을 위해 공격 트리와 사용 및 남용 사례를 구축한다. PASTA는 주요 의사결정권자를 참여시키고 운영, 거버넌스, 아키텍처 및 개발 부서의 보안 입력을 요구함으로써 위협 모델링 프로세스를 전략적 수준으로 끌어올린다. 궁극적으로 PASTA는 위협 열거 및 점수 매기기의 형태로 자산 중심의 결과를 생성하고, 힘들고 광범위한 과정을 돕기 위해 방법에 대한 매우 풍부한 문서가 개발되어 있다. PASTA는 기술 측면의 분석에만 국한되지 않고, 조직의 비즈니스 맥락을 통합적으로 고려함으로써 실제로 조직에 큰 영향을 미칠 수 있는 위험에 중점을 맞추고, 다양한 이해관계자들이 협업하여 실질적인 보안강화와 위험관리에 기여할 수 있도록 설계되어 있다.[25)]

3.2.6 VAST 위협 모델링

VAST (Visual, Agile, and Simple Threat) 위협 모델링은 2015년 Anurag Agarwal이 개발하였으며, 그가 운영 중인 위협 모델링 자동화 플랫폼인 ThreatModeler를 기반으로 한다. VAST는 애자일, 데브옵스 및 대규모 시스템 환경을 위한 방법으로 자동화와 시각화 도구를 활용하여 전통적인 위협 모델링 방법론의 복잡성을 감소시키고, 확장성과 민첩성을 높이는데 중점을 둔다. VAST는 애플리케이션 위협 프로필(Application Threat Profile) 및 운영 위협 프로필(Operational Threat Profile)과 같은 2가지 주요 관점을 통합하여 개발 및 운영 환경에 자연스럽게 통합될 수 있도록 설계되어 있다.

기본 요소	설명
자동화(Automation)	자동화를 통하여 반복적인 위협 모델링 수동작업을 제거함으로써 시간을 단축시키고, 지속적인 위협 모델링을 통해 기업 전체로 확장함
통합(Integration)	SDLC 전체의 도구와의 통합과 Agile DevOps 프로세스를 지원함
협업(Collaboration)	애자일 협업 도구를 통해 개발자, 보안팀 및 경영진 등 주요 이해관계자가 소통 및 협업함

그림 12. VAST 위협 모델링의 핵심 개요

애플리케이션 위협 프로필(ATP)은 프로세스 흐름 다이어그램(Process Flow Diagram)을 사용하여 아키텍처 관점에서 시스템을 표현하는 반면, 운영 위협 모델(OTP)은 공격자 관점에서 데이터 흐름도(Data Flow Diagram)를 기반으로 작성함으로써 위협 식별 및 분석 과정을 간소화하게 된다. 또한, 애플리케이션 위협 프로필(ATP)은 소프트웨어 애플리케이션 자체의 보안 속성과 위협에 초점을 맞추며, 데이터 흐름, 신뢰 경계, 인증 메커니즘 등 애플리케이션의 핵심 보안 요소를 시각화할 수 있는 반면, 운영 위협 프로필(OTP)은 애플리케이션이 배포되고 운영되는 환경의 보안 속성과 위협을 다루며, 네트워크 구성, 서버 배치, 클라우드 서비스, 액세스 제어 등의 운영 측면을 분석한다. 따라서 VAST는 소프트웨어 자체의 보안뿐만 아니라 운영 환경과 인프라의 보안까지 포괄적으로 고려할 수 있게 한다.[25)]

3.2.7 기타 위협 모델링 방법론

3.1 항에서 설명한 위협 모델링 방법론 이외에도 CVSS, Attack Trees, Persona non Grata, hTMM 및 Quantitative Threat Modeling Method 등과 같은 다양한 방법론을 선택할 수 있고, 단독으로 사용하거나 다른 위협 모델링 방법론과 결합하여 사용할 수 있다. 위험, 보안 또는 개인정보보호와 같이 특정 영역을 목표로 하는지, 위협 모델링에 사용할 수 있는 소요기간 및 비용, 위협 모델링에 대한 경험수준 및 이해관계자의 현실가능한 참여율 등을 고려하여 소프트웨어에 가장 적합한 위협 모델링 방법론을 결정해야 한다. 아울러, 위협 모델링 방법론은 스프린트의 기간과 모델링 반복 빈도에 따라 애자일 환경에서 모두 사용할 수 있다.[25)]

(1) Common Vulnerability Scoring System (CVSS)

CVSS는 소프트웨어 취약성의 주요 특성을 이해하고, 심각도를 정량적인 수치로 점수화하여 평가하는 기법이다. CVSS의 현재 버전인 4.0은 2023년에 출시되었으며, FIRST (FORUM of Incident Response and Security Teams)에서 관리되고 있다. CVSS는 사용자에게 다양한 사이버 및 사이버-물리적 플랫폼 내 공통적이고 표준화된 채점 시스템을 제공하고, CVSS 점수는 온라인에서 사용할 수 있는 계산기를 통해 산정할 수 있다. CVSS 4.0은 이전 버전인 CVSS 3.1의 한계를 보완하고, 실제 위협 환경을 보다 현실적으로 반영하도록 개선되었다. 기본(Base), 위협(Threat), 환경(Environmental) 및 보충(Supplemental) 총 4가지 메트릭 그룹으로 구성되어 있으며, 각 메트릭 그룹은 취약점의 본질적 특성, 시간에 따라 변하는 위협요소, 조직별 환경특성 및 추가적인 취약점 특성 등을 체계적으로 반영한다. 특히, 공격 성공에 필요한 사전 조건을 별도로 평가하는 Attack Requirements (AT) 항목이 새롭게 도입되었으며, 운영 기술(OT) 및 IoT 환경에서의 물리적 안전성 등도 평가 범위에 포함되어 다양한 산업 분야의 보안 요구사항을 충족할 수 있도록 개선되었다. 또한 점수 산정기준과 가이드라인이 좀 더 명확해져 평가자 간의 일관성을 높였으며, 점수 명명법을 구체화하였다. CVSS 4.0은 기존의 단순 점수 중심 평가에서 벗어나, 공격 현실성, 환경 맥락, 보안 대응 수준 등을 종합적으로 고려함으로써 조직이 보다 효과적인 위험기반 대응전략을 수립할 수 있도록 지원할 수 있도록 개선되었다.

(2) Attack Trees

Attack Tree는 1991년 Edward D. Weiss가 초기 제시하였으며, 1999년 Bruce Schneier에 의해 체계적으로 제안된 모델링 기법이다. 공격자의 목표 달성을 위한 모든 공격 경로를 트리(Tree) 형태로 시각화하고 구조화하는 방식으로 노드(node), 간선(edge)과 커넥터(connector) 등으로 구성되어 있다. Attack Tree의 루트 노드(root node)는 공격자의 최종 목표를 나타내고, 하위의 각 노드는 최종 목표를 달성하기 위한 공격 방법을 나타낸다. 개별 공격 목표인 각 노드는 하위 공격 목표 또는 상위 목표를 달성하는 수단인 자식 노드로 분해되며, 간선(edge)은 공격의 전이 상태를 나타내고, OR과 AND 커넥터(connector)로 2개 이상의 자식 노드들을 가진 노드의 공격목표 달성을 위한 전제 조건으로 나뉜다. 자식 노드 중 1개만 선택하여 실행이 가능한 경우인 OR 조합으로 나타낼 수 있고, 모든 자식노드가 반드시 실행되어야 상위 노드가 실행되는 경우인 AND 조합으로 나타낸다. Attack Tree는 정량적 또는 정성적 위협 모델링에 모두 활용할 수 있고, 공격자 중심의 관점에서 복잡한 공격과정을 논리적이고 계층적으로 시각화하여 파악할 수 있다는 도구라고 할 수 있다. 단, Attack tree에서 각 노드의 가중치를 부여하지 않은 한계점이 존재하고, 각각의 노드마다 위협의 정도가 모두 동일하지 않아 위협으로 인한 피해 정도가 상이한 점을 고려하지 않고, 발생 빈도 등을 고려하지 않으므로 보안 위협의 정도를 수치화하여 표현하기에는 한계점이 있다고 평가받고 있다.

(3) Persona non Grata

페르소나 논 그라타(Persona non Grata, PnG)는 미국의 디폴 대학교(DePaul University)에서 개발되었으며, 공격자 중심(Actor-centric)의 관점에서 악의적 페르소나의 동기, 자원과 기술 수준을 중점으로 사용자를 소프트웨어를 악용할 수 있는 원형으로 규정하고, 분석가가 의도치 않은 사용의 관점에서 소프트웨어를 바라보도록 한다. 이는 상대방의 위협을 시각화 하는데 도움이 되며, 위협 모델링 초기 단계에 도움이 될 수 있다. PnG 기법의 핵심은 잠재적 공격자의 프로파일을 식별하여 소프트웨어의 취약점과 침해 지점을 선제적으로 파악할 수 있도록 하는 것이다. PnG는 비교적 도입하기 쉽지만, 거의 사용되거나 연구되지 않았으며, 오탐률이 낮고 일관성이 높지만 특정한 위협 유형만 식별하는 경향이 있고 데이터 흐름이 복잡한 경우 적용 효율성이 감소하는 한계가 있다.

(4) Hybrid Threat Modeling Method (hTMM)

하이브리드 위협 모델링(hTMM)은 2018년 카네기 멜론 대학교의 소프트웨어 공학 연구소(Software Engineering Institute, SEI)에서 개발했으며, SQUARE (Security Quality Requirements Engineering Method) 방식, 보안 카드(Security Card) 및 페르소나 논 그라타(PnG) 등을 결합한 포괄적인 기법이다. hTMM은 가능한 모든 위협을 식별하고, 오탐(false positive)이 없고, 수행자와 관계없이 일관된 결과를 제공하고, 비용 효율적인 위협 모델링을 가능하게 하도록 설계되었다. hTMM의 주요 단계는 우선 위협 모델링을 적용할 소프트웨어를 식별하고, 보안 목표 및 자산을 명확하게 정의한 다음, 개발자의 제안에 따라 보안 카드를 적용하여 협업적 위협 시나리오를 제안한다. 이후 가능성이 낮거나 현실적으로 공격 벡터를 식별할 수 없는 페르소나 논 그라타(PnG)를 검증하여 제거하고, 도구 지원을 활용하여 결과를 요약한 후 공식적인 위험평가 방법을 계속 수행하게 된다. hTMM은 각 단일 위협 모델링 방법론의 한계를 극복하고, 보다 폭넓은 위협 커버리지와 분석의 일관성을 제공할 수 있다. 또한, 자동화 도구와 수동 분석을 병행적으로 사용함으로써 재현성을 높여 조직별 맞춤형 위협 모델링에 적합하다는 특징을 가진다.

(5) Quantitative Threat Modeling Method

Quantitative Threat Modeling Method는 Attack Tree, STRIDE 및 CVSS 방법론을 하이브리드 방식으로 통합한 정량적 위협 모델링 방법론이다. 2016년 미국 펜실베이니아주 피츠버그에서 열린 HotSoS2 컨퍼런스에서 Bradley Potteiger, Goncalo Martins 및 Xenofon Koutsoukos가 처음으로 소개하였으며, 사이버 물리 시스템의 복잡한 상호의존성을 고려한 정량적이고 체계적인 위협분석 접근방식에 해당한다. Quantitative Threat Modeling Method는 먼저 STRIDE의 Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service와 같은 5가지 위협 범주에 대해 각 구성요소 마다 Attack Tree를 작성하고, Common Vulnerability Scoring System 방법을 적용하여 공격 트리의 각 구성 요소에 대한 정량적 위험점수를 산출하고, 개별 구성 요소에 대한 공격 포트를 생성한다. Quantitative TMM의 핵심적인 특징 중 하나는 공격 포트(Attack port)를 정의하는 것인데, 공격 포트는 구성 요소별 공격 트리의 루트 노드로서 위험이 연결된 다른 구성 요소로 전달될 수 있는 진입점을 의미한다. 만약 공격 포트가 높은 CVSS 점수를 가진 구성 요소에 의존하는 경우, 해당 공격 포트 역시 높은 위험 점수를 가지며 공격 성공

가능성이 크다고 판단한다. 반대로 위험 점수가 낮은 구성 요소에 연결된 공격 포트는 상대적으로 낮은 위험도를 가진다. Quantitative Threat Modeling Method는 구성 요소 내 취약점의 심각도와 공격 가능성을 반영하며, 체계적인 위험 평가를 지원할 수 있다.

(6) TRIKE 위협 모델링

TRIKE 위협 모델링은 2005년 Brenda Larcom과 Elana Olson에 의해 개발되었으며, 위험기반 접근방식과 방어적 관점에서 소프트웨어와 관련된 행위자, 자산 및 의도된 행동 및 규칙을 열거하여 이해함으로써 보안 요구사항 모델을 구축한다. TRIKE는 행위자-자산-행동 매트릭스(Actor-Asset-Action Matrix)를 생성하는데, 이때 매트릭스의 열은 자산 집합을 나타내고, 행을 행위자를 나타낸다. 행위자-자산-행동 매트릭스의 각 셀은 CRUD(Create, Read, Update, Delete)와 같은 4가지 행동에 따라 나누어져야 하며, 각 행동에 대해 허용된 행동, 허용되지 않은 행동, 규칙이 적용된 행동 중 하나의 값을 할당해야 하고, 각 셀에는 규칙 트리를 첨부하며 보안 요구사항 정의가 완료되면 데이터 흐름도(DFD)을 작성한다. 각 구성요소는 특정 행위자 및 자산 집합과 매핑되고, DFD를 반복적으로 확인하고 위협을 식별하는데 이때 위협은 권한 상승(elevation of privilege) 또는 서비스 거부(denial of service) 두 가지 범주 중 하나에 속한다. TRIKE에서 식별된 각 위협은 공격 트리의 루트 노드가 되고, 자산에 대한 공격 위험도를 평가하기 위해 CRUD을 기준으로 각 행동별로 5단계 척도를 사용한다. 이는 해당 행동이 발생할 확률을 기준으로 한다. 행위자는 자산에 대해 가질 수 있는 위험도를 5단계 척도로 평가받으며, 숫자가 낮을수록 위험이 높다. 또한 각 자산에 대해 각 행동을 수행할 가능성을 3차원 척도(항상, 때때로, 절대 없음)로 평가한다. 단, TRIKE의 척도는 다소 모호하여 공식적인 방법론으로 보기 어렵다는 비판도 있으며, TRIKE 2.0 버전은 제대로 유지 관리되고 있지 않아 해당 웹사이트는 운영 중이지만, 관련 문서화가 되어 있지 않아 활용하기에 한계가 있다.

3.3 CIA Triad 확장모델 및 위협모델링 기반의 프레임워크

3.3.1 하이브리드 사이버보안 프레임워크

본 연구에서는 3.1장에서 소개한 확장된 CIA Triad 모델 및 3.2장에서 설명한 위협 모델링 방법론을 통합하여 소프트웨어 의료기기(SaMD)의 수명주기 전반에 걸쳐 적용할 수 있는 하이브리드 사이버보안 프레임워크(hybrid Cybersecurity Framework, hCSF)를 제안한다. 아래 <표6>와 같이 다양한 구성으로 이루어진 프레임워크가 출력될 수 있으며, 이를 효과적으로 적용하기 위해서는 해당 소프트웨어 의료기기(SaMD)의 의도된 사용목적(Intended use), 작용원리(Principle of operation) 뿐만 아니라 조직적 특성, 의료기기 및 사용환경의 특성과 외부 및 규제 환경의 특성 등을 전반적으로 고려하여 소프트웨어 의료기기(SaMD) 제조회사에서 자유롭게 선택하고 활용할 수 있도록 설계하였다. 구체적인 고려사항 및 활용방안은 3.4.1 사이버보안 프레임워크 적용 시 고려사항과 3.4.2 사이버보안 프레임워크 활용방안을 통해 제시하였다.

<table>
<tr><th>확장된 CIA Triad 모델</th><th>위협 모델링 방법론</th><th>하이브리드 사이버보안
프레임워크 예시</th></tr>
<tr><td rowspan="2">(A) Parkerian Hexad</td><td>(1) STRIDE</td><td rowspan="6">예. (B)(2) 프레임워크:
(McCumber Cube) +
(LINDDUN)
또는
(A)(1)(5) 프레임워크:
(Parkerian Hexad) +
(STRIDE + VAST)</td></tr>
<tr><td>(2) LINDDUN</td></tr>
<tr><td rowspan="2">(B) McCumber Cube</td><td>(3) OCTAVE</td></tr>
<tr><td>(4) PASTA</td></tr>
<tr><td rowspan="2">(C) 기타 보안목표 모델</td><td>(5) VAST</td></tr>
<tr><td>(6) 기타 기법</td></tr>
</table>

표 6. 하이브리드 사이버보안 프레임워크(hCSF)의 설계방식

본 연구에서 제안하는 하이브리드 사이버보안 프레임워크(hCSF)는 기본적으로 기술적인 사이버보안 요구사항 중심의 체크리스트 방식이 아닌 소프트웨어 의료기기(SaMD)의 수명주기 동안 지속적으로 활용할 수 있는 기술적, 관리적 및 운영적 측면의 사이버보안 요구사항을 식별하고, 대응할 수 있는 접근방식에 해당된다. 확장된 CIA Triad 모델을 통해 끊임없이 변화하는 새로운 기술 및 비즈니스

요구사항과 복잡한 사이버위협 환경에 대응할 수 있는 한층 강화된 보안목표 모델을 토대로 다양한 위협 모델링 방법론을 통합적으로 설계하여 소프트웨어 수명주기의 초기 단계부터 효과적인 사이버보안 대응전략을 마련할 수 있다. 대표적인 위협 모델링 방법론들은 3.2장에서 소개된 바와 같이 각각의 고유한 특징과 적용범위 등에 차이가 있다. 현재 가장 널리 사용되는 기법인 STRIDE 위협 모델링은 위장, 변조, 부인, 정보 유출, 서비스 거부, 권한 상승의 6가지 위협 유형을 통해 일반적인 보안 위협을 분석하며, 직관적인 사용방법으로 소프트웨어 설계 및 개발 초기단계에 적합하나 복잡한 소프트웨어에서는 위협의 수가 급격히 증가하는 한계가 있다. LINDDUN 위협 모델링은 특히 개인정보보호에 특화된 기법으로 연결성, 식별성, 부인 방지, 탐지성, 정보 공개, 인식 부족, 규정 미준수의 7가지 위협 유형을 6단계의 프로세스를 통해 분석하여 효과적이지만 많은 업무량과 시간이 소요될 수 있다.

구분	STRIDE	LINDDUN	OCTAVE	PASTA	VAST
주요 특징	일반적 보안위협	개인정보 보호	조직 위험관리	공격 시뮬레이션	애자일 자동화
적용 범위	소프트웨어 설계	데이터 보안	조직 전체	비즈니스 및 기술	개발 및 운영
복잡도	중간	높음	높음	매우 높음	낮음
시간 소요	중간	높음	높음	높음	낮음
자동화 수준	낮음	낮음	낮음	중간	높음

표 7. 대표적인 위협 모델링 방법론의 유형별 비교

OCTAVE 위협 모델링은 조직 차원의 위험관리 기법으로 운영 리스크, 보안 관행, 기술의 3가지 핵심요소를 기반으로 조직평가, 기술평가, 위험식별 및 전략 개발의 3단계를 통해 조직의 정보보안 거버넌스 수립에 효과적이나 방대한 문서화와 많은 시간투자가 필요할 수 있다. PASTA 위협 모델링은 공격 시뮬레이션 기반의 접근방식으로 7단계에 걸쳐 비즈니스 목표와 기술적 요구사항을 통합하여 실질적인 공격 가능성과 영향을 평가할 수 있고, 고도화된 위협분석에 유용하지만 복잡도가 매우 높고, 광범위한 과정으로 인해 많은 자원이 요구된다. VAST 위협 모델링은 Agile 환경에 특화된 기법으로 애플리케이션 위협 프로필과 운영 위협 프로필의 2가지 관점을 통합하여 자동화와 시각화 도구를 활용함으로써 전통적 위협 모델링의 복잡성을 감소시키고 확장성과 민첩성을 높였으나 특정한 플랫폼에 대한 의존성과

상대적으로 짧은 검증기간을 거친 방법론이라는 한계를 가지고 있다. 따라서 본 연구의 하이브리드 사이버보안 프레임워크(hCSF)의 주요 단계로써 소프트웨어 의료기기(SaMD) 제조회사는 우선 각각의 확장된 CIA Triad 모델 및 위협 모델링 방법론의 특성을 식별하고, 내부의 보안 목표와 자산을 명확하게 정의한 다음 수명주기 전반에 걸쳐 활용할 프레임워크를 전략적으로 설계한다. 이때, 반드시 단일의 위협 모델링 방법론을 선택하여야 하는 것은 아니며, 2개 이상의 위협 모델링 방법론을 결합해서 활용할 수 있다. 이후 설계한 하이브리드 사이버보안 프레임워크(hCSF)를 통해 소프트웨어 의료기기(SaMD)의 설계 및 개발 초기 단계부터 보안 요소를 고려하는 Security by Design 원칙을 구현하고, 가능한 모든 사이버보안 위협을 식별하고, 대응전략을 마련할 수 있다.

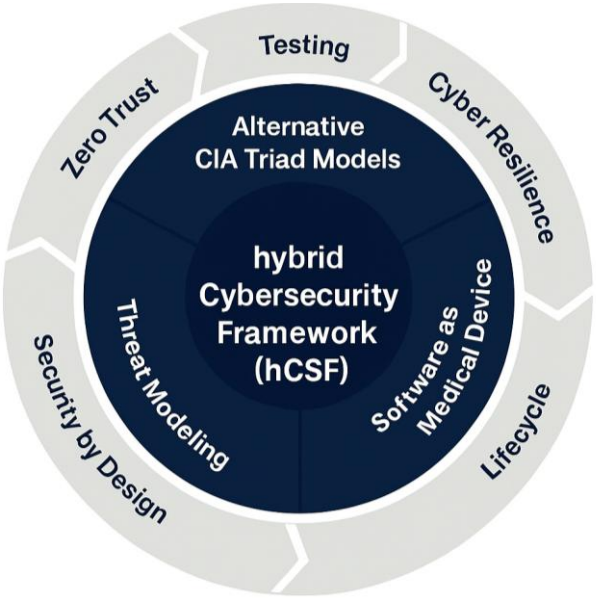

그림 13. 하이브리드 사이버보안 프레임워크(hCSF)

본 연구에서 제안한 하이브리드 사이버보안 프레임워크(hCSF)는 <그림13>과 같이 기존의 CIA Triad와 단일 위협 모델링 방법론 적용의 한계를 극복하고, 한층 더 폭넓은 사이버보안 위협 커버리지를 포함하고, 거시적 관점의 사이버보안 위험관리를 소프트웨어 의료기기(SaMD) 제조회사가 선택적으로 결합하여 제품의 수명주기 전반에 걸쳐 설계함으로써 조직별 맞춤형 사이버보안 시스템에 적합하다는 특징을 가진다.

3.3.2 하이브리드 사이버보안 프레임워크 예시

본 연구에서 제안한 하이브리드 사이버보안 프레임워크(hCSF)를 활용하여 설계한 예시로써 여러 확장된 CIA Triad 모델과 위협 모델링 방법론 중에서 McCumber Cube와 LINDDUN Threat Modeling을 선택적으로 결합하였다. 기본적으로 McCumber Cube 모델은 기밀성, 무결성 및 가용성과 같은 보안 목표(Security Goals)와 전송, 저장 및 처리와 같은 정보 상태(Information State) 그리고 기술, 정책과 관행, 교육훈련과 같은 보안 조치(Security Measures)라는 3가지 축으로 구성된 3차원 큐브 형태의 모델이다. 보안 위협 또는 취약점, 대응방안 등을 다각도로 분석하기에 적합하다. 한편, LINDDUN위협 모델링은 개인정보 보호분야에 중점을 두고 있기 때문에 개인 의료데이터와 관련된 보안을 위해 활용하기 적합하다. 연결성(Linkability), 식별성(Identifiability), 부인 방지(Non-repudiation), 탐지성 (Detectability), 정보 공개(Disclosure of information), 인식 부족(Unawareness), 규정 미준수(Non-Compliance)와 같은 7가지 위협 유형에 대해 6단계의 프로세스를 따르는 방식이며, 개인정보 보호통제를 위한 체계적인 접근방식을 제공한다. 따라서 (B)(2) McCumber Cube + LINDDUN 프레임워크는 사이버보안 및 개인정보보호를 동시에 만족할 수 있으며, <그림14>와 같이 크게 3가지 단계의 프로세스로 이루어진다.

첫번째 단계는 소프트웨어 의료기기(SaMD)의 작동 방식과 데이터 처리과정에 관한 공통되고 통합된 이해를 수립하기 위해 데이터 흐름도(DFD)를 활용하여 소프트웨어 시스템 외부의 사용자, 의료진, 환자 또는 제3자 서비스와 같은 외부 엔터티와 환자 기록, 진단 결과 등과 같은 개인 의료데이터를 저장하는 컨테이너 또는 서버, 데이터 분석, 진단 처리 등과 같은 알고리즘, 소프트웨어 시스템의 내부 또는 외부의 정보 전파 경로와 같은 데이터 흐름의 4가지 핵심 요소를 구조화되고 표준화된 그래픽 방식을 시각화한다. 소프트웨어 의료기기(SaMD) 제조회사는 데이터 흐름도(DFD)를 통해 소프트웨어의 전체적인 아키텍처를 시각적으로 명확하게 파악하고, 논리적 구분을 표시하는 신뢰 경계를 설정하여 보안 도메인 간의 경계와 잠재적 취약점을 식별할 수 있다. 이때, McCumber Cube의 정보 상태에 해당하는 전송, 저장 및 처리 상태를 활용하여 환자의 개인 의료데이터에 관해 수명주기 전반에 걸쳐 보안 위협을 최대한 식별하는 것이 중요하다.

두번째 단계에서는 해당 소프트웨어 의료기기(SaMD)에서 식별된 모든 보안 위협과 첫 단계에서 정의한 데이터 흐름도(DFD)를 반복적인 분석을 통합 맵핑

작업을 수행하여 개인 의료데이터의 수집, 전송, 저장 및 분석 처리하는 과정에서 발생할 수 있는 개인정보보호 및 사이버보안과 관련된 위협을 심층적으로 식별한다. LINDDUN 위협 모델링의 공개된 매핑 테이블을 사용하여 각 소프트웨어 구성요소의 조합에 관해 고려해야 할 구체적인 LINDDUN위협 유형을 체계적으로 식별하고, 매핑 테이블에서 중요도가 높다고 표시된 조합들에 대해서는 LINDDUN 위협 트리를 활용하여 실제 소프트웨어 의료기기(SaMD)가 운용되는 환경에서 발생 가능한 구체적이고 현실적인 사이버보안 위협 시나리오를 구성한다. 이를 통해 식별된 모든 위협들과 특성 등을 문서화하여 재검토 시 효과적으로 추적할 수 있도록 구축한다.

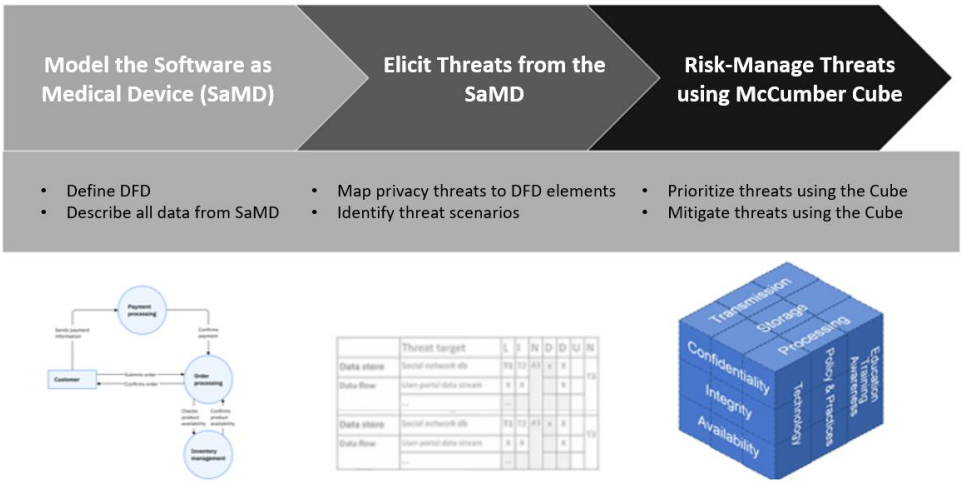

그림 14. (B)(2) McCumber Cube + LINDDUN 프레임워크 프로세스

최종 단계에서는 McCumber Cube를 활용하여 식별된 모든 사이버보안 위협들에 대한 우선순위를 설정하고, 보안 위협에 대응하는 완화전략을 수립한다. McCumber Cube의 보안 목표를 기준으로 각 보안 위협이 소프트웨어 의료기기(SaMD)와 환자 안전에 미치는 잠재적 영향도와 발생 가능성을 평가한다. 또한, McCumber Cube의 보안 조치를 기준으로 암호화 및 접근제어 등과 같은 기술, 보안 관련 정책 및 관행, 이해관계자 대상 사이버보안 및 개인정보보호 교육훈련 및 인식제고를 통합적으로 고려한 대응전략을 수립하고, 문서화하고 소프트웨어 수명주기 전반에 걸쳐 이 3가지 단계의 프로세스는 일관되고 반복적인 방식으로 지속 이행하여야 한다.

3.4 CIA Triad 확장모델 및 위협모델링 기반의 프레임워크 적용

3.4.1 프레임워크 적용 시 고려사항

본 연구에서 제안한 확장된 CIA Triad 모델과 위협 모델링 방법론을 기반으로 한 소프트웨어 의료기기(SaMD)의 사이버보안 프레임워크를 효과적으로 적용하기 위해서는 조직적 특성, 의료기기 및 사용환경의 특성과 외부 및 규제 환경의 특성 등을 고려해야 한다. 먼저, 조직적 특성을 고려한 접근방식 (Organizational Consideration)이 요구된다. 스타트업, 중견기업 또는 글로벌 대기업 등과 같이 조직 규모 및 보안 성숙도 등에 따라 요구되는 사이버보안 정책, 보안전략 목표 및 프레임워크의 적용범위가 상이하므로 사전적 검토가 필요하다. 사이버보안 목표의 우선순위와 적용범위를 조직의 특성에 맞게 최적화하고, 기존의 품질경영시스템과 본 연구의 사이버보안 프레임워크를 연계하여 사이버보안을 별도의 프로세스가 아닌 품질경영시스템의 일부로써 통합적으로 적용함으로써 프로세스 간 중복요소를 최소화하고 효율성을 극대화해야 한다. 또한, 조직 내 보안 성숙도, 정보보안책임자와 같은 사이버보안 전문인력 보유 여부와 보안 서비스 전문기업의 활용가능성은 프레임워크의 실행력을 결정하는 핵심적인 요소이므로 적용 시 반드시 고려해야 한다.

둘째, 의료기기 또는 사용환경의 특성을 고려한 접근방식(Software as Medical Device or Use environment-specific Consideration)이 요구된다. 소프트웨어 의료기기(SaMD)는 일반적으로 의료용 빅데이터를 인공지능(AI)으로 분석하여 질병을 진단, 관리하거나 예측하여 의료인의 업무를 보조하는 소프트웨어 또는 의학적 장애나 질병을 예방, 관리 및 치료하기 위해 환자에게 근거기반의 치료적 개입을 제공하는 소프트웨어를 포함하며, 각 소프트웨어 의료기기 (SaMD)의 사용목적, 작용원리 및 아키텍처 등이 상이하므로 사전적 검토가 필요하다. 또한, 소프트웨어 의료기기(SaMD)는 상급종합병원, 종합병원 및 병원 또는 환자의 일상환경 등과 같이 다양한 사용환경에서 사용될 수 있으며, 진료기록, 의료영상, 생체신호, 병리검사, 유전정보 등과 같은 민감한 의료데이터를 수집, 전송, 저장 및 분석 처리하는 기능을 가지고 있어 적절한 프레임워크를 설계하여 사이버보안 중심의 제품 개발 프레임워크(Secure Product Development Framework, SPDF)를 소프트웨어 설계 및 개발 단계, 배포 단계, 유지보수 단계 및 폐기 단계까지 수명주기 전반에서 보안 요소를 고려하여 적용해야 한다.

마지막으로 사이버보안 프레임워크 적용 시 외부 환경 및 규제 환경의 특성을 고려한 접근방식(Consideration on External and Regulatory Environment)이 요구된다. 소프트웨어 의료기기(SaMD)는 전자의무기록시스템 (Electronic Medical Record, EMR), 의료영상저장전송장치(Picture Archiving and Communication System, PACS) 또는 병원정보시스템(Hospital Information System, HIS) 등 다양한 외부 시스템과 연동되어 상호운용성(Interoperability)를 위한 사이버보안 통제가 요구되고, 점차 더 복잡한 기술 환경에 의존하고 있으며, 이로 인한 사이버보안 위협의 수가 급격히 증가하고 있다. Zero-Day Attack 등과 같은 신종 취약점의 등장과 생성형 인공지능(AI) 등을 이용한 새로운 형태의 사이버 공격으로 인해 기존의 경계기반 사이버보안 접근방식으로는 대응할 수 없는 새로운 보안위협 환경을 최대한 고려하여 프레임워크를 검토해야 한다. 또한, 소프트웨어 의료기기(SaMD) 제조회사는 출시하고자 하는 관할 국가의 사이버보안 규제정책 및 가이던스에 따른 보안 정책, 보안 목표 및 사이버보안 요구사항 등을 사전에 고려해야 한다. 국내 식약처 또는 미국 식품의약국(FDA) 등과 같은 각국의 규제기관은 고유한 사이버보안 요구사항에 대한 준수를 요구하고 있으므로 각국의 공통적인 사이버보안 요구사항을 추출하여 프레임워크 내 호환가능한 보안 요소를 검토해서 최적화된 프레임워크를 선택해야 한다.

3.4.2 사이버보안 프레임워크 활용방안

본 연구에서 제안한 확장된 CIA Triad 모델과 위협 모델링 방법론을 기반으로 한 소프트웨어 의료기기(SaMD) 사이버보안 프레임워크를 효과적으로 활용할 수 있는 방안은 다음과 같다. 먼저, 소프트웨어 의료기기(SaMD)의 위협 모델링을 효과적으로 시각화하기 위해 데이터 흐름도(Data Flow Diagram), 상태 다이어그램(State Diagram), 스윔 레인 다이어그램(Swim Lane Diagram) 등 여러 형태의 다이어그램을 활용할 수 있다. 둘째, 글로벌 시스템 뷰(Global System View), 다수 환자 위해 뷰(Multi-Patient Harm View), 보안 사용 사례 뷰(Security Use Case View) 등과 같은 보안 아키텍처 뷰를 통해 소프트웨어 의료기기 (SaMD)의 모든 엔드포인트 간 보안 분석을 포함하여 시스템 수준의 분석을 활용할 수 있다. 셋째, 소프트웨어 의료기기(SaMD) 제조회사가 선택한 위협 모델링 방법론과 함께 AAMI TIR57: 2016 Principles for medical device security – Risk management등에 따라 사이버보안 위험관리 프로세스를 기존의 품질경영시스템에 통합하여 활용할 수 있다. 마지막으로 사이버보안 테스트 (Cybersecurity

Testing)을 통해 적용한 프레임워크의 효과성을 입증하기 위한 기본적인 취약성 테스트(Vulnerability Testing), 퍼즈 테스트(Fuzz Testing), 침투 테스트(Penetration Testing) 및 고급 보안분석 시험 등을 활용할 수 있다.[11)19)24)]

(1) 다이어그램(Diagram)

본 연구를 통해 제안된 사이버보안 프레임워크를 소프트웨어 의료기기(SaMD)에 적용하는 경우 위협 모델링을 효과적으로 시각화하기 위한 데이터 흐름도(Data Flow Diagram), 상태 다이어그램(State Diagram), 스윔 레인 다이어그램(Swim Lane Diagram) 등과 같은 다이어그램을 활용할 수 있다. 데이터 흐름도(Data Flow Diagram, DFD)는 위협 모델링 시스템을 시각화하는 대표적인 도구이며, 소프트웨어 의료기기(SaMD)의 주요 기능과 관련된 엔터티들과 엔터티들 간의 관계, 신뢰 경계(Trust Boundary)를 상위 수준에서 표현하여 소프트웨어의 전체적인 구조를 파악하는 데 효과적이다. 상태 다이어그램(State Diagram)은 소프트웨어의 상태변화나 통신 프로토콜과 같은 동적 상호작용을 평가할 때 더욱 적합한 다이어그램이며, 소프트웨어의 워크플로우를 도식화하고 추가적인 조사가 필요한 가정들을 식별하는 데 유용하다. 스윔 레인 다이어그램(Swim Lane Diagram)은 여러 컴포넌트가 협력하여 목표를 달성하는 과정을 포착하는 데 유용하며, 분석 프로세스 뿐만 아니라 의사결정 플로우차트 작성에도 활용되어 각 참여 주체의 역할과 책임을 명확히 구분할 때 활용할 수 있다. 따라서 다이어그램은 소프트웨어 의료기기(SaMD)의 전체적인 시스템에서 사이버 위협의 발생위치를 식별하고 공격경로를 시각적으로 추적할 수 있는 도구이며, 사이버 위협과 소프트웨어 구성요소에 고유식별자를 부여해 외부문서와 연계하고 완화조치를 추적하는데 유용하게 활용할 수 있다.

(2) 아키텍처 뷰(Architectural View)

본 연구를 통해 제안된 사이버보안 프레임워크를 소프트웨어 의료기기(SaMD)에 적용하는 경우 글로벌 시스템 뷰(Global System View), 다중 환자 위해 뷰(Multi-Patient Harm View), 보안 사용 사례 뷰(Security Use Case View) 등과 같은 보안 아키텍처 뷰를 활용하여 소프트웨어 의료기기 (SaMD)의 보안 위협에 대응하기 위한 보안통제 수단이 어떻게 적용되었는지를 구조적으로 파악할 수 있다.

글로벌 시스템 뷰(Global System View)는 소프트웨어 의료기기(SaMD)의 아키텍처에 대한 종합적인 관점을 제공하며, 소프트웨어 의료기기(SaMD)와 모든 내·외부 연결을 포함하여 소프트웨어 업데이트 인프라, 네트워크 및 클라우드 연결 등과 같은 모든 연결요소를 식별할 수 있다. 다중 환자 위해 뷰(Multi-Patient Harm View)는 소프트웨어 의료기기(SaMD)와 네트워크에서 발생할 수 있는 동시 다발적 손상 가능성을 다루며, 하나의 손상이 발생시키는 사이버보안 위험을 통해 여러 환자에게 미칠 수 있는 보안 위험을 평가하는데 활용할 수 있다. 보안 사용 사례(Security Use Case View)는 보안으로 인한 손상이 소프트웨어 의료기기(SaMD)의 안전성이나 유효성에 영향을 미칠 수 있는 모든 기능에 대한 다양한 운영 및 기능 상태를 평가하며, 소프트웨어 의료기기(SaMD)의 사이버보안 복잡성과 위험에 따라 확장된다. 또한, 업데이트 및 패치가능성 뷰(Updatability and Patchability View)는 소프트웨어 의료기기(SaMD) 수명주기 전반 동안 보안 위협에 대응하기 위한 신속하고 신뢰할 수 있는 업데이트를 제공하는 엔드포인트 간의 프로세스를 파악하는데 활용할 수 있다. 따라서 보안 아키텍처 뷰는 소프트웨어 의료기기(SaMD)의 복잡한 사이버보안 위협에 대응하기 위해 다양한 관점에서 보안 통제의 적용을 구조적으로 파악하고 평가할 수 있는 체계적이고 포괄적인 분석도구로 유용하게 사용할 수 있다.

(3) 사이버보안 위험관리(Cybersecurity Risk Management)

본 연구를 통해 제안된 사이버보안 프레임워크를 소프트웨어 의료기기(SaMD)에 적용하는 경우 소프트웨어 의료기기(SaMD) 제조회사가 선택한 위협 모델링 방법론과 함께 AAMI TIR57: 2016 Principles for medical device security Risk management등에 따라 사이버보안 위험관리 프로세스를 기존의 품질경영시스템에 통합하여 활용할 수 있다. 소프트웨어 의료기기(SaMD)의 상호운용성 증가로 인해 사이버보안 위험관리가 소프트웨어 설계 및 개발 초기 단계에서부터 중요한 과제로 대두되고 있으며, 사이버보안 중심의 제품 개발 프레임워크(Secure Product Development Framework, SPDF)을 활용하여 소프트웨어 의료기기(SaMD)의 수명주기 전반에 걸쳐 사이버보안 위험관리를 합리적으로 수행할 수 있다. 본 연구에서 제시한 하이브리드 사이버보안 프레임워크(hCSF)와 같은 자체적인 프레임워크 내에서도 통합하여 효과성을 극대화할 수 있다. 또한, 소프트웨어 의료기기(SaMD)의 사이버보안 위험관리를 효율적으로 운용하기 위해서는 소프트웨어의 안전 및 보안과 관련된 위험을 해당

소프트웨어 의료기기(SaMD)가 운용되는 상위 개념의 전체적인 시스템 맥락에서 접근해야 하며, 사이버보안 위협과 공격 기술이 끊임없이 발전하는 특징을 고려하여 어떠한 소프트웨어 의료기기(SaMD)도 완전히 안전할 수 없다는 일종의 제로 트러스트(Zero Trust) 보안 모델의 원칙을 적용하여 사이버보안 위험관리 프로세스를 품질경영시스템에 통합하여 수명주기 전반에 걸쳐 활용할 수 있다.[26)]

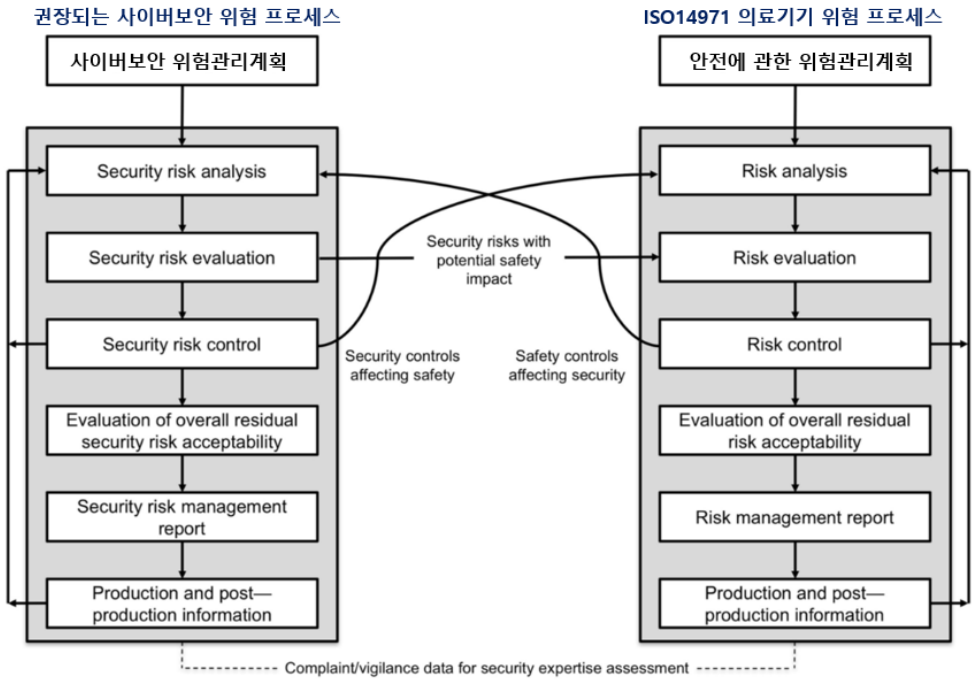

그림 15. 사이버보안 위험관리와 의료기기 위험관리 프로세스의 관계도

사이버보안 위험관리는 ISO 14971:2019 Medical devices – Application of risk management to medical devices에 설명된 의료기기의 안전에 관한 위험관리와 구별된다. 의료기기의 안전에 대한 위험관리는 환자의 물리적 손상이나 치료지연에 중점을 두는 반면, 의료기기 사이버보안에 대한 위험관리는 직간접적인 환자 피해와 기업의 비즈니스 또는 평판 위험까지 포함하고 있다. 따라서 소프트웨어 의료기기(SaMD) 제조회사는 의료기기의 안전과 사이버보안에 관한 위험관리를 본 연구에서 제시한 프레임워크 등을 활용하여 모두 수행할 수 있다. 소프트웨어 의료기기(SaMD)는 알려진 취약점을 제거하거나 완화하도록 설계 및 개발되어야

하며, 이미 시판된 소프트웨어 의료기기(SaMD)의 경우 설계 완화가 불가하다면 보상 통제를 고려하도록 한다. 알려진 취약점이 부분적으로만 완화되거나 완화될 수 없는 경우, 합리적으로 예측가능한 위험으로 평가되어 추가적인 통제조치나 사용자에게 위험 전가를 검토할 수 있도록 한다. 소프트웨어 의료기기(SaMD)의 사이버보안 위험관리 활동을 본 연구의 사이버보안 프레임워크 등을 연계하는 경우, 국내외 의료기기 규제준수에 요구되는 위협 모델링, 사이버보안 위험평가, 소프트웨어 자재명세서(Software Bill Of Materials, SBOM), 취약점 또는 미해결 이상평가 등과 같은 문서화 프로세스에도 활용할 수 있다.[11)27)]

(4) 사이버보안 시험(Cybersecurity Testing)

본 연구를 통해 제안된 사이버보안 프레임워크를 소프트웨어 의료기기(SaMD)에 적용하는 경우 지속적인 사이버보안 시험(Cybersecurity Testing)를 수행하여 프레임워크의 효과성을 입증하기 위한 기본적인 취약성 테스트(Vulnerability Testing), 퍼즈 테스트(Fuzz Testing), 침투 테스트(Penetration Testing) 및 고급보안 분석시험 등을 활용할 수 있다. 사이버보안 시험은 소프트웨어 의료기기(SaMD)의 보안 취약점을 사전에 식별하고 평가하는 핵심적인 과정이며, 소프트웨어 의료기기(SaMD) 뿐만 아니라 보안 절차, 내부 통제, 인간 행동 또는 구현에서 악용될 수 있는 취약점을 파악하는데 사용한다. 취약성 테스트(Vulnerability Testing)은 오용사례 분석, 형식오류 및 예상치 못한 입력에 대한 견고성 검증, 공격표면 분석, 취약점 연쇄분석, 알려진 취약점 스캐닝 등과 같은 코드분석 평가를 말하며, 퍼즈 테스트(Fuzz Testing)은 소프트웨어 의료기기(SaMD)에 의도적으로 형식이 잘못되거나 예상치 못한 데이터 또는 호출 시퀀스를 입력하여 입력 검증오류, 버퍼 오버플로우, 메모리 누수 등의 결함을 자동화된 방법으로 발견하는 평가방법이다. 침투 테스트(Penetration Testing)는 사이버 공격을 시뮬레이션하여 소프트웨어 의료기기(SaMD)의 보안 취약점을 실증 테스트하는 평가방법이다. 이외에도 제3자 시험기관을 활용한 보안분석 시험 등을 활용할 수 있으며, 사이버보안 시험에서 발견된 오류 또는 이상점은 보안 위험관리 프로세스의 관점에서 평가되어야 하며, 기능적 영향이 미미하더라도 악용 가능성이 있다면 보안상 더 큰 피해를 야기할 수 있기 때문에 반드시 완화조치를 취해야 한다.

4 결과

본 연구에서는 확장된 CIA Triad 모델과 위협 모델링 방법론을 기반으로 소프트웨어 의료기기(SaMD)의 수명주기 전반에 걸쳐 활용할 수 있는 하이브리드 사이버보안 프레임워크(hCSF)를 개발하였다. 개발된 프레임워크는 기존의 전통적이고 획일화된 의료기기 위험관리 접근방식에서 벗어나 Parkerian Hexad 모델 및 McCumber Cube 모델 등의 CIA Triad 확장모델과 STRIDE, LINDDUN, OCTAVE, PASTA 및 VAST Threat Modeling 등과 같은 다양한 위협 모델링 방법론을 통합하여 설계되었으며, 소프트웨어 의료기기(SaMD)의 의도된 사용목적, 작용원리 및 진출하고자 하는 국가의 사이버보안 규제정책 또는 조직의 보안정책 등에 따라 다양한 결합으로 구성될 수 있는 유연성을 제공한다. 특히 진료기록, 의료영상, 생체신호, 병리검사, 유전정보 등과 같은 민감한 개인 의료데이터를 수집, 전송, 저장 및 분석 처리하는 소프트웨어 의료기기(SaMD)의 특성을 고려하여 환자의 개인정보보호와 환자안전이라는 핵심 보안 요구사항을 동시에 실현할 수 있도록 설계되었으며, 설계 및 개발 초기 단계부터 보안 요소를 고려하는 Security by Design 원칙을 구현할 수 있어 품질비용 측면에서 효율적이고 효과적인 보안체계 구축을 가능하게 한다.

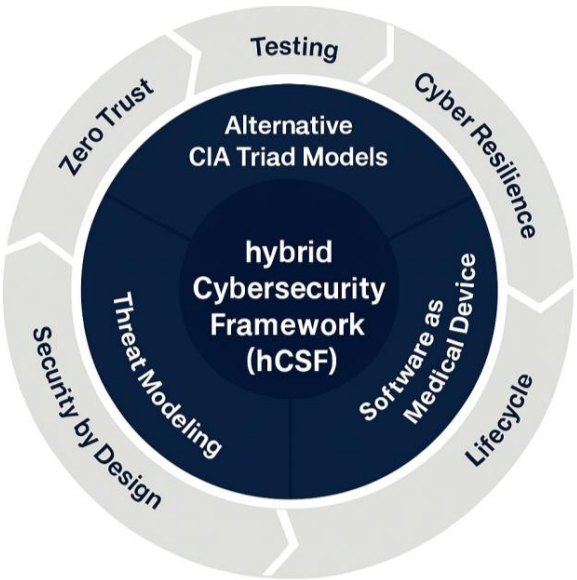

그림13. 하이브리드 사이버보안 프레임워크(hCSF)

5 고찰

본 연구에서는 확장된 CIA Triad 모델과 위협 모델링 방법론을 기반으로 소프트웨어 의료기기(SaMD)의 수명주기 전반에 걸쳐 활용할 수 있는 사이버보안 프레임워크를 제시하였으며, McCumber Cube모델 및 LINDDUN Threat Modeling을 적용한 하이브리드 사이버보안 프레임워크(hCSF)를 통해 실제 환경에서 적용 가능할 수 있는 활용 사례로 소개하였다. 본 연구의 결과로써 소프트웨어 의료기기(SaMD)의 의도된 사용목적, 작용원리 및 진출하고자 하는 국가의 사이버보안 규제 또는 조직의 보안 정책 등에 따라 다양한 결합으로 구성된 하이브리드 사이버보안 프레임워크(hCSF)가 출력될 수 있으며, 특히 진료기록, 의료영상, 생체신호, 병리검사, 유전정보 등과 같은 민감한 개인 의료데이터를 수집, 전송, 저장 및 분석 처리하는 소프트웨어 의료기기 (SaMD)의 특성을 고려할 때, 환자의 개인정보보호 및 환자 안전이라는 핵심적으로 요구되는 보안 및 소프트웨어 요구사항을 동시에 실현하는데 효과적일 것으로 기대된다. 본 연구를 통해 제안한 소프트웨어 의료기기(SaMD)의 사이버보안 프레임워크는 설계 및 개발 초기 단계부터 보안 요소를 고려하는 Security by Design 원칙을 구현할 수 있도록 지원하기 때문에 품질비용 측면에서도 효율적이고, 보안체계를 효과적으로 구축할 수 있을 것으로 기대된다. 조직의 규모에 크게 상관없이 유연하게 적용할 수 있는 프레임워크로서 조직의 내부 자원과 전문성에서 제약이 있는 대다수의 소프트웨어 의료기기(SaMD) 제조회사에서도 보다 체계적인 사이버보안 거버넌스를 수행할 수 있는 사이버보안 프레임워크를 제공할 수 있을 것이다. 소프트웨어 의료기기(SaMD)의 경우, 설계 및 개발 단계, 배포 단계, 유지보수 단계 및 폐기 단계의 수명종료 프로세스까지 수명주기 전반에서 보안 요소를 고려해야 하므로 이러한 하이브리드 형태의 사이버보안 프레임워크를 통해 보안 시스템을 강화하는데 활용할 수 있다.

한편, 본 연구에는 몇 가지 한계점이 존재하며, 이를 보완하기 위한 향후 후속 연구가 필요하다. 우선 본 연구를 통해 제안한 소프트웨어 의료기기(SaMD)의 사이버보안 프레임워크는 현재 이론적으로 설계된 방법론적인 모델로서 실제 상용 중인 소프트웨어 의료기기(SaMD)에 적용한 이후에 품질관리 측면에서의 효율성 및 비용효과성에 관한 검증 결과가 포함되어 있지 않으며, 각 의료기관의 IT 기반시설 및 소프트웨어 의료기기(SaMD) 제조회사의 보안 성숙도 등에 따라 사이버보안 프레임워크의 적용 가능성과 효과성에서 편차가 있을 수 있다. 또한, 본 연구에서 제안된 사이버보안 프레임워크를 통한 접근방식은 소프트웨어 의료기기(SaMD)를 대상으로 제한적으로 고안되었으며, 모든 유형의 의료기기에 동일하게 적용하기

어려우며, 그 실효성을 보장하기는 어렵다. 예컨대 종속형 소프트웨어(Software in Medical Device, SiMD) 등과 같은 의료기기 소프트웨어 유형에 대한 추가적인 검증이 필요할 것이다. 마지막으로 본 연구에서 제안된 사이버보안 프레임워크는 소프트웨어 설계 및 개발 단계에서의 전략적인 보안목표 및 위협 모델링 설계에 중점을 두고 있어 실제적인 운영 환경에서 발생할 수 있는 실시간 사이버 공격이나 위협에 대한 대응 메커니즘이 상대적으로 부족할 수 있다. 따라서 Zero-Day Attack 등과 같은 신종 취약점 또는 최근 새롭게 등장한 생성형 AI등을 이용한 사이버 공격에 대한 즉각적인 대응전략이 추가적으로 필요하고, 의료기기 분야의 사이버보안에 관한 국제 표준과 각국의 규제 또한 지속적으로 발전하고 있기 때문에 본 연구에서 제안된 프레임워크가 이러한 변화를 모두 반영하기에는 한계가 있다. 따라서 향후 연구에서는 한계점을 보완하여 더욱 포괄적이고 실시간 위협대응 전략도 가능한 하이브리드 사이버보안 프레임워크(hCSF)를 발전시킬 필요가 있으며, 궁극적으로 본 연구에서 제시한 사이버보안 프레임워크를 통해 소프트웨어 의료기기(SaMD)의 수명주기 전반에서 발생가능한 사이버보안 위협을 식별 및 대응관리하고, 위험기반 접근방식의 보안 제품설계를 통한 사이버 복원력을 강화하는 데 유용한 프레임워크를 제공하여 점차 복잡해지는 사이버보안과 관련된 국내 및 해외 규제심사나 시장진입에 필요한 문서화 요건을 충족하는 데에도 기여할 것이다.

6 결론

최근 국내 대기업들의 대규모 사이버 공격 사태가 연이어 발생하면서 사이버 보안에 대한 사회적 경각심이 고조되고 있다. 국내 모 통신사의 해킹 사고와 인스턴트 메신저 회사의 데이터센터 화재로 인한 플랫폼 마비 사태는 디지털 초연결 사회의 취약성을 여실히 드러냈으며, 정보통신기술(IT) 기업에 맡겨진 인프라 기능의 보안 체계가 얼마나 허술한 지 보여주었다. 사이버보안 전문가들은 최근 발생한 사태들을 계기로 편리성을 위해 IT 기업들에 상당한 부분을 위탁한 현대 사회의 인프라 기능의 위협과 취약성을 재검토하고, 정보보호 관련법규 및 조직의 내부통제 등과 같은 제도적 기반을 한층 강화할 필요가 있다고 지적한다. 국회입법조사처는 특히 보안 관련 고위험 산업군에 대한 강화된 인증기준 적용과 보안 전문가 협의회 심의에 대한 의무화 등의 법령 개정 필요성을 제언하였으며, 선진적인 방식도입 등의 중요성을 강조하고 있다. 본 연구는 디지털 전환이 가속화되는 상황에서 확장된 CIA Triad 모델과 위협 모델링 방법론을 활용하여 소프트웨어 의료기기(SaMD)의

수명주기 전반에 걸쳐 적용할 수 있는 하이브리드 사이버보안 프레임워크(hCSF)를 제안하였다. 기존의 전통적이고 획일화된 의료기기 위험관리 접근방식에서 벗어나 Parkerian Hexad및 McCumber Cube 모델 등과 같은 확장 모델과 STRIDE, LINDDUN, PASTA, OCTAVE, VAST Threat Modeling 등과 같은 다양한 위협 모델링 방법론을 활용함으로써 소프트웨어 의료기기(SaMD)의 기술적, 관리적 및 운영적 측면의 보안 요구사항을 고려한 수명주기 전반에 걸친 대응전략을 구현할 수 있는 프레임워크 및 활용방안을 마련하였다.

또한 디지털 헬스케어 시대의 도래와 함께 소프트웨어 의료기기(SaMD)의 활용이 급증하고 있는 상황에서 환자 안전과 개인정보보호를 위한 체계적인 사이버보안 프레임워크는 사실상 선택사항이 아닌 필수사항이라고 할 수 있다. 2023년 의료 분야의 데이터 유출로 인한 평균 피해액이 1,093만 달러에 달하고 13년 연속 피해액 규모가 최고치를 기록하고 있는 현실은 의료기기 분야에서 사이버보안이 가지는 중요성과 시급성을 여실히 보여준다고 할 수 있다. 본 연구는 이와 같은 문제를 타개하기 위한 하이브리드 사이버보안 프레임워크(hCSF)를 제안하였다는 점에서 다음과 같은 의의 및 성과가 있다. 첫째, 본 연구의 사이버 보안 프레임워크를 통해 Parkerian Hexad 모델 및 McCumber Cube 모델 등을 포함한 CIA Triad 확장모델을 토대로 소프트웨어 의료기기(SaMD)에 대한 사이버 공격을 구조적으로 위협 모델링하고, 사이버보안 위협과 취약점을 수명주기 전반에 걸쳐 평가하고 모니터링 관리할 수 있는 새로운 관점의 접근방식을 제안하였다는 점이다. 둘째, 본 연구의 사이버보안 프레임워크를 통해 기존의 기술적 보안 요구사항 체크리스트를 넘어서 소프트웨어 의료기기(SaMD)의 수명주기 동안 지속적으로 활용할 수 있는 품질경영시스템 측면에서의 고려사항을 반영한 맞춤형 사이버보안 전략을 수립할 수 있도록 새로운 방향성을 제시하였다는 점이다. 마지막으로 본 연구의 사이버보안 프레임워크를 통해 Security by Design 원칙을 실행할 수 있도록 소프트웨어 의료기기(SaMD)의 초기 설계 및 개발 단계부터 사이버보안 요소를 고려하는 사전 예방적 접근방법을 통해 사후 대응적 접근방법보다 비용 효율적이고 효과적인 보안체계를 구축하는 방안을 마련하였다는 점이다. 따라서 본 연구를 통해 확장된 CIA Triad 모델과 위협 모델링 방법론 기반의 사이버보안 프레임워크 활용은 소프트웨어 의료기기(SaMD) 사이버보안 연구분야의 새로운 이론적 접근방식을 도출하였으며, 향후 관련 연구의 기초 자료로 활용할 수 있을 것으로 기대된다.

아울러, 소프트웨어 의료기기(SaMD) 제조회사에서 본 연구를 통해 제안된 사이버보안 프레임워크 등을 활용한 보안 거버넌스 체계를 소프트웨어 의료기기(SaMD) 수명주기 동안 구축하고, 사이버보안 중심의 제품개발 프레임워크(Secure Product Development Framework, SPDF) 프로세스를 실현하기 위해서는 품질경영시스템 내 일종의 소프트웨어 의료기기(SaMD)를 위한 사이버보안 책임자(Chief Cybersecurity Officer for Software as Medical Device)를 지정하도록 권장하는 제도적 근거를 마련할 필요가 있으며, 부족한 사이버보안 전문인력 또는 재원확보 문제 등으로 인해 지정이 불가피한 경우에는 정부 차원에서 안랩, 시큐아이, 이글루시큐리티 등과 같은 국내 정보보호 전문서비스 기업 또는 보안관제 전문기업 지정제도에 따른 사이버보안 전문기업과 소프트웨어 의료기기(SaMD) 제조회사 간의 전략적 파트너십 구축을 제도적으로 지원할 필요가 있다. 소프트웨어 의료기기(SaMD) 제조회사는 각국 정부, 산업계 또는 학계와의 지속적인 협력 및 지원을 통해 핵심 경쟁력인 사이버보안을 내재화하여 가상 세계에서 창과 방패처럼 끊임없이 진화하는 보안 위협에 대응하여 지속적인 혁신과 연구가 요구됨을 시사한다.

마지막으로 사이버보안은 개인, 기업 또는 국가의 안전과 직결되는 분야로써 단순한 기술적인 과제를 넘어 사회 전반의 안전과 신뢰를 결정짓는 중대한 사안이다. 특히 소프트웨어 의료기기(SaMD)는 환자의 민감한 개인정보와 의료데이터를 사용하기 때문에 사이버 공격의 주요 표적이 되고 있으며, 사이버 공격으로 인한 피해는 경제적인 손실을 넘어 환자에게 심각한 상해 또는 사망, 영구적 장애 또는 손상을 초래할 수 있다는 부분에서 매우 중대하게 다루어야 할 과제이다. 소프트웨어 의료기기(SaMD)는 의료기기 산업의 대표적인 미래성장동력으로 글로벌 산업 경쟁력을 높이고, 선제적으로 우위를 확보하기 위해서는 사이버보안 역량강화가 불가피하며, 앞으로 인공지능, 차세대통신 및 양자컴퓨팅 등과 같은 신기술이 끊임없이 발전하면서 급증할 사이버 위협과 공격에 대비하여 전략적, 기술적, 조직적 준비태세가 필요하다. 따라서 소프트웨어 의료기기(SaMD) 제조회사는 새로운 사이버보안 프레임워크를 도입하고, 보안기술 연구개발에 대한 투자와 노력을 확대해야 하며, 정부와 학계는 이러한 소프트웨어 의료기기(SaMD) 제조회사를 적극적으로 지원하여 의료기기 산업 전반의 사이버보안 수준 향상을 도모해야 할 것이다. 본 연구가 향후 소프트웨어 의료기기(SaMD)의 사이버보안 프레임워크 정책수립에 기초 연구자료로 활용되어 한층 더 안전하고 신뢰할 수 있는 디지털 헬스케어 및 소프트웨어 의료기기(SaMD)의 보안 생태계 구축에 조금이나마 기여할 수 있기를 기대한다.

참고문헌

1. IQVIA, Digital Health Trends 2024, 2024
2. Market.US, Software as a Medical Device (SaMD) Market Research Report, 2024
3. Food and Drug Administration (FDA), Medical Device Cybersecurity Helping to Keep Patients and Medical Devices Safe, 2023
4. International Medical Device Regulators Forum (IMDRF), IMDRF/CYBER WG/N60: Principles and practices for medical device cybersecurity, 2020
5. The Health Insurance Portability and Accountability Act Journal, 2024 Healthcare Data Breach Report, 2025
6. 조상진, 사이버보안 산업 동향 및 시사점, KDB산업은행 미래전략연구소, 2023
7. 김주람, KISTI R&I Report: 사이버보안 과학기술 · 산업분석, 한국과학기술정보연구원, 2024
8. 식품의약품안전처, 의료기기의 사이버보안 허가·심사 가이드라인(민원인 안내서), 2025
9. IBM Corporation, Cost of a Data Breach Report 2024, 2024
10. Michael E Whitman, Herbert J. Mattord, Principles of Information Security 4th ed., Cengage Learning, 2012
11. FDA, Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions
12. European Commission, MDCG 2019-16 Guidance on Cybersecurity for medical devices, 2020
13. International Medical Device Regulators Forum (IMDRF), IMDRF/CYBER WG, IMDRF/CYBER WG/N73: Principles and practices for software bill of materials for medical device cybersecurity, 2023
14. International Medical Device Regulators Forum (IMDRF), IMDRF/CYBER WG/N70: Principles and practices for the cybersecurity of legacy medical devices, 2023
15. National Institute of Standards and Technology (NIST), SPECIAL PUBLICATION 1800-26A, 2020

16. Arnbak, A.M., Securing private communications: Protecting private communications security in EU law: fundamental rights, functional value chains and market incentives, Universiteit van Amsterdam, 2015
17. John McCumber, Assessing and Managing Security Risk in IT Systems: A Structured Methodology, 1st ed, Auerbach Publications, 2004
18. 이경복, 박태현, 트럼프 2기 행정부의 미국 사이버보안 정책방향 전망, SW중심사회, 소프트웨어정책연구소, 2025
19. Food and Drug Administration (FDA), Select Updates for the Premarket Cybersecurity Guidance: Section 524B of the FD&C Act, 2024
20. Food and Drug Administration (FDA), Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff, 2016
21. 고은아, 김홍빈, 김진규, 윤주연, EU의 디지털 미래 구축을 위한 사이버보안(Cybersecurity) 방향과 시사점 – 사이버보안 입법 동향을 중심으로, 한국인터넷진흥원, 2023
22. 과학기술정보통신부, 12대 국가전략기술, 대한민국 기술주권 책임진다, 2022
23. 식품의약품안전처, 디지털의료기기 전자적 침해행위 보안지침 제정고시, 2025
24. MITRE CORPORATION, Medical Device Innovation Consortium, Playbook for threat modeling medical devices, 2021
25. Shevchenko, N., et al., Threat modeling: A summary of available methods. Carnegie Mellon University, Software Engineering Institute, 2018
26. AAMI TIR57: 2016 Principles for medical device security Risk management
27. ISO 14971:2019 Medical devices – Application of risk management to medical devices
28. 과학기술정보통신부, 민관합동조사단 SKT 침해사고 관련 민관합동조사단 중간조사 결과, 2025

ABSTRACT

A Cybersecurity Framework for Software as a Medical Device: Integrating Alternative CIA Triad Models and Threat Modeling Methodologies

This research is purposed to suggest a novel cybersecurity framework to strengthen security of Software as a Medical Device (SaMD), whose use has rapidly increased with the advent of the digital healthcare era. As cybersecurity threats continue to rise, highlighted by an average financial loss of $10.93 million per data breach in the healthcare sector, marking the highest figure for 13 consecutive years, the importance and urgency of cybersecurity in the SaMD domain have become more prominent. This research introduces a hybrid Cybersecurity Framework (hCSF) that can be applied throughout the entire lifecycle of SaMD, based on the alternative CIA Triad model and threat modeling methodologies. The proposed framework integrates CIA Triad models expanded such as the Parkerian Hexad and McCumber Cube, along with various threat modeling approaches including STRIDE, LINDDUN, and OCTAVE. This integration enables comprehensive management of cybersecurity requirements from technical, administrative, and operational perspectives. By implementing the principle of Security by Design, the framework would facilitate the inclusion of security considerations from the early stages of software design and development, offering a more cost-effective and efficient security approach compared to reactive methods. The study confirms that the proposed framework can be flexibly configured into various combinations tailored to the intended use, principle of operation, and cybersecurity regulatory policies of the target market for SaMD. Moving beyond the traditional checklist approach to technical cybersecurity requirements, this study presents a new framework that identifies cybersecurity threats and implements response strategies throughout the SaMD lifecycle. It provides a new theoretical perspective and direction in the field of SaMD cybersecurity. Ultimately, the research aims to contribute to the improvement of global competitiveness in the SaMD sector, serve as a foundational reference for cybersecurity policy development, and support the establishment of safer and more reliable digital healthcare and SaMD cybersecurity management strategies.

Keywords: Medical Device; Software as Medical Device; Cybersecurity; Threat Modeling Methodology; Framework; Lifecycle; CIA Triad; SaMD; Security by Design